МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
СТАРООСКОЛЬСКИЙ ТЕХНОЛОГИЧЕСКИЙ ИНСТИТУТ ИМ. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения
высшего образования
«Национальный исследовательский технологический университет «МИСиС»

МИСиС
Старооскольский технологический
институт имени А.А. Угарова

ВСЕРОССИЙСКАЯ НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ КОНФЕРЕНЦИЯ С МЕЖДУНАРОДНЫМ УЧАСТИЕМ «ЛОМОНОСОВСКИЕ ЧТЕНИЯ - 2021»

ТОМ I

8 апреля 2021 г.
г. Старый Оскол

УДК 378:001.891
ББК 74.48:72.5
В85

Материалы Всероссийской научно-исследовательской конференции с международным участием «Ломоносовские чтения – 2021» под редакцией А.В. Боевой, г.Старый Оскол: СТИ НИТУ «МИСиС», 2021 - I том, 687с.

Сборник содержит статьи Всероссийской научно-исследовательской конференции с международным участием «Ломоносовские чтения – 2021» преподавателей, обучающихся образовательных организаций общего, среднего профессионального и высшего образования Российской Федерации и зарубежных стран.

Всероссийская научно-исследовательская конференция посвящена 310-летию со дня рождения М.В. Ломоносова, основателя российской науки, выдающегося русского ученого, филолога, историка, поэта. На конференции рассмотрены возможности информационно-коммуникационных технологий в науке и на производстве; перспективы и проблемы цифровой трансформации образования: инновационные технологии в преподавании; роль социально-воспитательной среды в формировании компетентного специалиста. Материалы отражают содержание научно-исследовательской, опытно-конструкторской деятельности преподавателей и обучающихся за 2020-2021 учебный год.

Сборник предназначен для преподавателей и обучающихся образовательных организаций разного уровня.

Направление 1

Возможности современной студенческой проектной, исследовательской и научной деятельности и её практическая реализация

Секция 1.1

ОСОБЕННОСТИ ОРГАНИЗАЦИИ ДЕЯТЕЛЬСТИ САМОЗАНЯТЫХ ГРАЖДАН

Арская Алина Сергеевна, студент 2-го курса
Научный руководитель Богданова Екатерина Николаевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС» Оскольский политехнический колледж, г. Старый Оскол

Самозанятые — категория налогоплательщиков, применяющая налоговый спецрежим «налог на профессиональный доход».

Налог на профессиональный доход подразумевает, что эти лица уплачивают налоги за свою профессиональную деятельность, т.е. они работают сами на себя без найма у работодателя и без привлечения дополнительного наемного труда по трудовым договорам. Налогом облагается сам труд и использование имущества самозанятого.

Самозанятость — работа непосредственно на заказчиков (физических и юридических лиц), а не работодателя по найму.

Еще в 2020 году самозанятость распространилась на все регионы России. С 1 июля можно получить возможность оформить спецрежим в возрасте 16 лет.

Основные формы самозанятости:

1.Частное (физическое) лицо без ИП.

2.Самозанятый ИП.

Гражданин РФ или стран ЕАЭС может стать плательщиком НПД, если:

1. Осуществляет свою деятельность на территории РФ из списка участвующих в эксперименте. Причем человек может либо сам находиться в таком регионе, либо выполнять работы для физических лиц и компаний из таких регионов. Оформление самозанятости доступно и гражданам Беларуси, Армении, Киргизии и Казахстана, если они сотрудничают с заказчиками из российских областей, где действует спецрежим.
2. Ведет свою деятельность один, без привлечения наемных работников.
3. Возраст – с 14 лет при условии согласия родителей, эмансипации или регистрации брака. С 18 лет дополнительных условий нет.
4. Доход не превышает 2,4 млн рублей в год. При этом неважно, ежемесячно самозанятый получает выручку или нет. Нет дохода – нет налога.
5. Получает доход только в денежной форме.

По основной работе большую распространенность имеет деятельность в качестве агента по недвижимости (риелтора), строителя, водителя, работника сельского хозяйства, сферы красоты или искусства

По дополнительной работе - деятельность в качестве репетитора, IT-специалиста или по оказанию юридических, финансовых, страховых услуг, ремонту бытовой или компьютерной техники, написанию каких-либо научных текстов

У каждого третьего самозанятого дополнительная работа не соответствует основной занятости. Тем, кто хочет использовать специальный налоговый режим, нужно зарегистрироваться в качестве налогоплательщика налога на профессиональный доход. Сделать это можно за считанные минуты с помощью нескольких инструментов: специального мобильного приложения «Мой налог»; кабинета налогоплательщика «Налога на профессиональный доход» на сайте ФНС; на портале Гослуги.

Однако проще всего использовать всё же мобильное приложение «Мой налог».

Алгоритм постановки на учет включает следующие этапы:

1. Отправка комплекта необходимых документов в налоговую:

- заявления о постановке на учет;

- копии паспорта и фотографии физлица (не требуются, если у гражданина РФ есть доступ в личный кабинет налогоплательщика на сайте ФНС или портале Госуслуг).

Заявление, копия паспорта, фотография физлица формируются с использованием мобильного приложения «Мой налог» (можно скачать из Google Play и App Store), и для этого не требуется усиленная квалифицированная электронная подпись.

2. Уведомление налогового органа поступает через мобильное приложение «Мой налог» — не позднее дня, следующего за днем направления заявления.

Налоговая вправе отказать в постановке на учет, если выявляются противоречия или несоответствия между представленными документами и сведениями, имеющимся у налогового органа (при этом налоговая указывает противоречия и предлагает повторно представить документы). Датой постановки на учет физического лица в качестве налогоплательщика является дата направления в налоговый орган соответствующего заявления. Иностранцы могут тоже зарегистрироваться через мобильное приложение «Мой налог», но только по ИНН. По паспорту регистрация будет недоступна.

Как уже было сказано выше, плательщики НПД не могут работать на работодателя и иметь сотрудников. Но при этом можно работать где-то и отдельно работать как самозанятый на кого-то другого. Нельзя работать на своего работодателя или бывшего работодателя, если с момента прекращения трудового договора не прошло 2 года.

Доход от деятельности самозанятого не может быть больше 200 тыс. руб. ежемесячно (плюс — минус), т.е. сумма не должна превышать 2,4 млн. руб. ежегодно.

Также ограничения распространяются на торговлю маркированными или подакцизными товарами (алкоголь, сигареты, одежда и обувь и др.).

Самозанятые не могут:

- заниматься перепродажами товаров или имущественных прав, кроме продажи личного имущества;
- заниматься добычей или продажей полезных ископаемых,
- иметь сотрудников;
- осуществлять деятельность в интересах третьих лиц по договорам поручения, комиссии или агентским договорам (кроме тех, кто оказывает услуги доставки и приему платежей в интересах третьих лиц);
- использовать другие налоговые режимы с НДФЛ.

При оформлении самозанятости необходимо уведомить налоговую о месте ведения деятельности. Если самозанятый работает в нескольких городах, то субъект можно выбрать самостоятельно. Изменить место можно только раз в год. Если в выбранном субъекте самозанятый больше не ведет свою деятельность, то он выбирает другой субъект в течение 30 календарных дней.

Для самозанятых предоставляются следующие льготы:

- Физические лица на НПД освобождаются от уплаты НДФЛ;
- Индивидуальные предприниматели на НПД освобождаются от НДФЛ, от НДС (кроме уплаты НДС при ввозе товара в Россию), страховых фиксированных платежей**.**

Также если в течение месяца вы не получили никакой доход, то никаких налогов платить не нужно. Плательщики НПД имеют право на оказание помощи по ОМС, так как участвуют в программе.

Налоги самозанятые уплачивают непосредственно с полученных доходов от продажи товаров или выполнения работ или услуг, реализации прав на имущество.

При этом налоги не начисляются на средства, полученные: по трудовому договору, при продаже недвижимости или машины, при передаче имущественных прав на недвижимость (кроме аренды жилья), от госслужащих, кроме доходов от сдачи жилья в аренду, от продажи личного имущества, при продажи доли в уставном капитале, паев в фондах кооперативов и инвестиционных фондах, ценных бумах и производственных финансовых инструментов, при работе в простом товариществе или по договору доверительного управления имуществом, в результате выполнения работ или оказания услуг

текущему или бывшему работодателю (не прошло два года), в результате деятельности по 70-му пункту 217 статьи Налогового кодекса РФ, если лицо состоит на учете в Налоговой по 7-му пункту 83 статьи того же кодекса, по переуступке прав требований, в натуральном виде, непосредственно от арбитражного управления, медиаторской или оценочной деятельности, работы нотариуса, адвокатской деятельности.

Самозанятый уплачивает 4 % в отношении доходов, полученных от реализации товаров или услуг физлицам, и 6 % — в отношении доходов, полученных от реализации товаров или услуг ИП (для использования при ведении предпринимательской деятельности) и юрлицам.

Налогоплательщик может настроить процесс уплаты налога таким образом, чтобы необходимая сумма списывалась с банковского счета. Для этого в мобильном приложении нужно предоставить налоговому органу право на направление в банк соответствующих поручений.

Налогоплательщик имеет право уменьшить налоговую базу в расчетном периоде за счет возврата ранее полученных сумм (например, при отказе от товара, работы или услуги со стороны заказчика) или ошибочно внесенной сделки в приложение “Мой налог”. Налог автоматически пересчитается.

Каждому самозанятому государство предоставляет налоговый вычет в размере 10 000 руб. Но он не выдается налогоплательщику, на эту сумму постепенно уменьшается налог на профессиональный доход.

Особенности:

1. Вычет дается один раз при регистрации.
2. Не нужно подавать заявление в налоговую инспекцию. Она сама учтет вычет при начислении налога.
3. Вычет снижает ставки до 3 % при получении денег от физлиц и до 4 % – от юрлиц и ИП.
4. В приложении “Мой налог” плательщик сразу увидит, сколько он уже исчерпал вычета, а сколько осталось. После того как все 10 000 руб. будут учтены в НПД, ставки вернутся к прежним размерам.
5. Вычет не сгорает в течение года, неиспользуемый остаток переносится на следующий и так далее годы.

Отдельного разговора заслуживает совмещение ИП и самозанятости. Работают все те же ограничения, представленные выше. Но чтобы перейти на спецрежим, индивидуальный предприниматель должен отказаться от используемого им налогового режима, потому что совмещать сразу два не получится.

Потребуется уведомить налоговую службу о переходе на уплату НПД. Срок – 1 месяц с момента регистрации в качестве налогоплательщика НПД. Если предприниматель не уложился в срок, то у него аннулируют статус самозанятого и он вернется к своему прежнему налоговому режиму.

Как и у любого налогового режима, у экспериментального есть свои плюсы и минусы.

Плюсы:

- легализация своего бизнеса без боязни проверок и санкций со стороны налоговой службы;
- можно совместить ИП и самозанятость;
- не надо вести бухгалтерию и подавать декларации;
- не надо покупать контрольно-кассовые аппараты для получения денег от клиентов;
- уплачивается только один налог по низким ставкам 4 и 6 %;
- страховые взносы во внебюджетные фонды не уплачиваются;
- получение налогового вычета в размере 10 000 руб.;
- простые регистрация и механизм работы с заказчиками через приложение;
- подходит для безработных граждан, женщин, пенсионеров, можно совмещать с другой работой;

- с НПД есть отчисления на обязательное медицинское страхование, поэтому плательщик имеет полное право пользоваться своим полисом ОМС и получать бесплатные медицинские услуги;

- возможность получить статус гражданам других государств, если они работают с клиентами из России.

Минусы:

- есть ограничения по видам деятельности и доходу;
- нельзя нанимать сотрудников;
- нельзя работать с бывшим работодателем, если со дня увольнения не прошло двух лет;
- нет отчислений в пенсионный фонд, придется копить на пенсию самостоятельно;
- режим пока действует до 2028 года, что будет с ним потом – неизвестно.

Самозанятый в 2021 году продолжат свое существование на тех же условиях. Планируется существенный прирост по количеству зарегистрировавшихся граждан. В 2021 году плательщиков налога на профессиональный доход (а именно предпринимателей) ждут проверки Налоговой. На настоящий момент ФНС уже разработала схемы выявления махинаций с применением нового налогового режима. Всех сомнительных предпринимателей, которые заменяют сотрудников самозанятыми, начнут проверять с начала года.

Список использованных источников

1. О проведение эксперимента по установлению специального налогового режима «Налог на профессиональный доход» [Электронный ресурс]: Федеральный закон №422-ФЗ от 27.11.2018г. (редакция от 08..2020г). Доступ из справ.-правовой системы «Консультант Плюс»
2. ИФНС России: официальный сайт. https://npd.nalog.ru/
3. Гос.услуги: официальный сайт. https://www.gosuslugi.ru/

РОЛЬ КСЕНОБИОЛОГИИ В ОСВОЕНИИ МАРСА

Атанов Денис Александрович, студент 1-го курса
Научный руководитель Киреева Людмила Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет МИСиС»
Оскольский политехнический колледж
город Старый Оскол

Гипотеза: ксенобиология поможет в освоении Марса.

Объект исследования: ксенобиология.

Предмет исследования: организмы, созданные ксенобиологами, а в частности организмы, которые смогут жить на Марсе.

Ксенобиология представляет собой подраздел синтетической биологии, изучающий создание и управление биологическими устройствами и системами. Она появилась не так давно и ещё не знакома науке. На практике это обозначает новые биологические и биохимические системы, которые отличаются от канонической системы **ДНК-РНК.** Например, вместо ДНК или РНК, взять, так называемый, ксенонуклеиновые кислоты (КсНК) в качестве носителей информации.

Потенциал этой науки заключается в возможности получить новые знания о биологии и происхождении жизни. Почему же жизнь развилась от РНК к системе ДНК-РНК-белок и её универсальному генетическому коду. Это эволюция или обычная случайность, или некие факторы исключили появление других типов химических систем?

Ксенобиология пытается посредством создания усиленных биополимеров воссоздать что-то новое, биополимеры — это класс полимеров, входящие в состав живых организмов. Полимеры—это неорганические и органические вещества, соединённых в длинные макромолекулярные связи. Это показывает, насколько наш мир может быть уникальным и неизведанным [1].

Целью ксенобиологии является проектирование и создание биологических систем, которые будут отличаться от своих природных аналогов. Новые организмы будут более совершенными в каждом возможном биохимическом аспекте, у них будет другой генетический код.

Ученые хотят выйти из природных рамок эволюции и изменить саму биохимическую основу жизни. Исследования в области ксенобиологии можно представить как:

- создание искусственной клетки (или протоклетки);
- создание искусственных аминокислот и белков;
- изменение генетических носителей ДНК и РНК.

Протоклетка — это примитивный организм, который возник из-за скопления органических веществ, он представляет собой примитивную форму жизни. Протоклетка или протобионт – это самоорганизующаяся структура, отделяющая внутреннее содержимое от внешнего мира, или другими словами структура подобная биологической клетке, с которой предположительно и начала формироваться современная жизнь на заре эволюции. Самый большой вопрос, который мучает ученых относительно этих простых структур – как они сформировались миллиарды лет назад и как эволюционировали в современные клетки.

В принципе, сейчас создать замкнутую сферическую структуру из липидной мембраны (ее уже можно считать простейшей протоклеткой) не сложно, а вот поместить в нее другие биологические молекулы, взаимодействующие друг с другом, чтобы проходили

сложные биохимические реакции, уже намного сложнее. Заставить делиться вновь созданные клетки, вообще задача на сегодняшний день трудно решаемая.

Вполне вероятно, в древние времена, когда протоклетки образовывались в большей степени случайно, а не благодаря сложным биологическим процессам, структурными единицами были не липиды, а жирные кислоты. Образуемая из них мембрана - менее прочная и легче проницаемая для органических молекул. На этом этапе эволюции в клеточной мембране есть много приспособлений для транспорта необходимых соединений внутрь и ненужных - наружу, а тогда примитивные живые организмы не имели такой возможности, поэтому приходилось выхватывать из потока, проходящего через протоклетку то, что можно было использовать. Например, сейчас люди живут в изолированных домах, когда нам что-то необходимо, мы покупаем это и приносим домой, а мусор выносим в мусорный контейнер. А теперь представьте, что местом для жизни людей становится центре урагана и в доме вместо окон большие дыры, и люди сидят дома и ждут пока нужные вещи просто влетят в окно, а ветер будет проносить сквозь него все, что попадается на его пути. Примерно так поступали протоклетки миллиарды лет назад, жизнь и потоки органики были хаотичны, поэтому клеточная мембрана была совсем другой [4].

Ксенобиология в перспективе освоения Марса играет важную роль!

Ксенобиология полностью поменяет наш мир и поможет в освоении других планет, например планеты Марс. Ученые могут создать клетку, которая будет комфортно себя чувствовать в среде обитания Марса.

Микроорганизм должен существовать при:

1. отсутствии кислорода,
2. отсутствии света.

Ученые могут создать протоклетку и попробовать поместить ее в условия такие же, как на Марсе, чтобы она могла вжиться в эту среду.

Оказывается подходящая клетка уже есть. Её обнаружили ученые из Томска Desulforudis audaxviator, она смогла бы жить на Марсе! Эту бактерию более десяти лет пытались найти исследователи разных стран.

У этого микроорганизма была выявлена структура, по мнению специалистов, обеспечивающая ему способность распространяться повсюду, например, газовые вакуоли, напоминающие плавательный пузырь рыб. По версии ученых, бактерия Desulforudis audaxviator может «путешествовать» по воздуху. Исследователи констатируют, что способность бактерии вырабатывать энергию для жизни в условиях полного отсутствия света и кислорода делает для нее возможным существование жизнь на Марсе. По словам микробиологов, обнаруженная бактерия скрывает механизм, который может быть связан с какими-то фундаментальными основами существования живых клеток, которые пока не изучены наукой.

Ксенобиологи смогут доработать эту клетку, чтобы она лучше приспособилась к жизни на Марсе.

Сейчас ученые конструируют протоклетки из различных липидов и жирных кислот, а затем изучают, какие молекулы и при каких условиях могут проходить внутрь. Таким образом, они стараются смоделировать живые организмы. Фактически, ученые ищут грань между еще не живыми органическими молекулами и живыми организмами.

В исследованиях простейших форм жизни участвуют не только ксенобиологи, но и астробиологи, так как благодаря подобным экспериментам можно оценить условия на планете, при которых способна зародиться жизнь и, следовательно, понять, где и по каким критериям стоит искать обитаемые планеты.

Искусственную клетку можно рассмотреть в двух аспектах: с одной стороны это может быть протоклетка, созданная из неживых молекул, с другой стороны это может быть организм, контролируемый искусственным ДНК. Уже в 2010 году было объявлено о создании первой искусственной клетки. Ученые взяли последовательность ДНК, переписали нативный генетический код и собрали его искусственно, после чего внедрили

его в клетку, предварительно лишенную родного ДНК. Клетка не только приняла чужеродные гены, но и начала синтезировать белки, а также размножаться [2].

А что будет, если попробовать изменить самые главные составляющие жизни – углерод и воду? Раздел ксенобиологии, изучающий альтернативную биохимию – ответит на этот вопрос.

Углерод – самый жизненно важный элемент Вселенной. Он может образовывать 4 связи, а также двойные и тройные связи, поэтому природа смогла создать огромное разнообразие органических молекул, что необходимо для жизни на Земле.

Лучший кандидат на замену углерода – кремний. Он тоже может образовывать 4 связи, но из-за своего гораздо большего размера, намного сложнее образует двойные и тройные связи, что необходимо для создания полимеров, особенно аналогов липидов. Это значительно сокращает потенциальное разнообразие кремне-органических молекул. Есть и еще один недостаток: аналог углекислого газа, диоксид кремния, чаще всего является твердым веществом, которое крайне трудно удалить из организма. Т.е. в кремневом мире из живых организмов песок будет сыпаться в прямом смысле слова. Встречается кремний в космическом пространстве гораздо реже. Но есть небольшой парадокс: на нашей планете кремния все-таки больше чем углерода, однако, жизнь у нас все равно углеродная. Может это связано с тем, что наши предки были занесены на планету извне, а может это свидетельствует о том, что углерод больше подходит для развития жизни. Но ученые продолжают искать следы кремневой жизни во Вселенной [3].

Рассматривается ряд теорий о жизни на основе фосфора, азота и бора, но они, как правило, носят совсем спекулятивный характер. Наиболее экзотический элемент, который может участвовать в формировании жизни – мышьяк. Долгое время такие теории даже не рассматривались, но в 2010 г. учеными из NASA не была обнаружена бактерия, которая активно использует мышьяк вместо фосфора.

Интересно, что воду как растворитель заменить легче, чем углерод, например, жизнь может зародиться в аммиачном океане (есть только один недостаток, такой океан при похолодании будет промерзать до дна). Еще один кандидат – метан и/или этан, купаться в такой маслянистой водичке вряд ли будет приятно, но для жизни, рожденной в ней, вполне подойдет.

Титан, спутник Сатурна, является одним из первых кандидатов на поиск внеземной жизни, а ледяные берега этого далекого мира омывают именно метан-этановые моря и реки. Ученым очень хочется найти теоретическое доказательство возможности существования там жизни.

Ученые нашей планеты все больше углубляются в альтернативную или искусственную жизнь. Это поможет осваивать новые планеты.

Ксенобиология – надежда космологов всего мира. Эта наука имеет все шансы на освоение планет, а в частности, Марса.

Список использованных источников

1. https://sunely-tales.livejournal.com/13615.html
2. https://wiki2.org/ru/Ксенобиология
3. https://myslide.ru/presentation/ksenobiologiya-i-biotestirovanie
4. https://wikichi.ru/wiki/Xenobiology

ГРАФОН КАК СПОСОБ ОБЩЕНИЯ В СОЦИАЛЬНЫХ СЕТЯХ

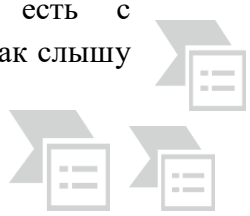
Атанов Денис Александрович, студент 1-го курса
Научный руководитель Капустина Ирина Владимировна, преподаватель
Оскольский политехнический колледж Старооскольского технологического института им. А.А. Угарова (филиала) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Социальные сети сегодня быстро отвечают на новые веяния в языке, поскольку являются синтезом различных стилей русского языка и наиболее быстро откликаются на любые перемены в речи. Наиболее часто подростки в своей речи стремятся использовать самые разнообразные средства передачи эмоций и информации. Самым универсальным средством сегодня является употребление стикеров в различных мессенджерах. Именно они наиболее красочно передают фонетические особенности речи и эмоции пишущего.

Необычное, мотивированное контекстом написание на фоне графического (или орфографического) стандартов называется ***графоном*** [4, с.106]. К графонам относят: написание прописных букв вместо строчных и наоборот, дефиксацию, факультативные кавычки, включение в графический облик слова элементов иных знаковых систем (цифры, буквы латинского алфавита), курсив, использование разных шрифтов, подчеркивание и т.д. [4, с.4].

Всем известно,что задача любого текста – передать некую информацию, донести ее до адресата. Устное сообщение всегда эмоционально. Но как же в письменном тексте передать эмоции? На сегодняшний день это довольно просто – в социальных сетях большую популярность набрали *стикерпаки* – наборы статичных или анимированных картинок, иногда с небольшими репликами. Цель их – не только эмоционально воздействовать на адресата, но и сэкономить время на написание сообщения.

Помимо реплик, написанных верно с точки зрения орфографии русского языка, большую популярность набирают стикеры с графонами, то есть с орфографическими ошибками, изменением графического облика слова («как слышу так и пишу»). Например: *«Моё увожение», «Удоли», «Подори», «Што ты мне сделаешь», «Нифкусна и грустна», «Не еш, подумой»* и т.п.



Почему же подобные стикеры пользуются большей популярностью, чем стикеры без ошибок? Под графоном понимается, как правило, отклонение от нормы, но подразумевается, что графоны выполняют выделительную функцию. Цель их – максимально доходчиво и эмоционально донести информацию от автора к читающему.

Тот или иной графон, автор не только привлекает внимание к содержанию сообщения, но и руководит процессом восприятия информации, как бы расставляя акценты в тексте, руководя его взглядом, останавливая его на необходимых словах [2].

Таким образом, стикер служит и для внешней организации оформления сообщения, и передает смысловую информацию. То есть ошибки, допущенные в стикерах передают эмоции пишущего и привлекают внимание на уровне подсознания – мы невольно обращаем внимание на внешний облик сообщения.

Также стикеры помогают «разгадать» эмоции пишущего, которые при чтении чаще всего трактуются неоднозначно. Картинка визуализирует авторские мысли, так сказать, является подтекстовой информацией. И чаще всего этот подтекст предстает в комической форме. Этим и объясняется использование таких стикеров, как *«я сделаль», «кушац», «хотю внимания», «неть», «дя»* и т.п. Комический эффект здесь достигается путем имитации детской речи. Использование таких стикеров, как *«ску-у-у-чна», «икскьюзьми», «намана», «палехчи», «вот это па-па-паворот»* и т.п. основано на приеме звукоподражания.

Проанализировав различные точки зрения ученых в области изучения комических текстов, мы пришли к выводу, что комическое всегда содержит подтекст - скрытую авторскую мысль.

Таким образом, постоянное расширение медиапространства, обилие каналов получения и передачи информации приводят к тому, что читатель выбирает самое интересное или самое важное в короткий промежуток времени, иными словами «то, что бросается в глаза». В таких условиях пишущий вынужден использовать средства визуализации, коими выступают стикерпаки, для достижения своей цели при донесении информации. Таким образом, стикеры на сегодняшний день – это необходимость, а стикеры-графоны – это еще и прагматизм.

Список использованных источников

1. Анохина Т.О. О полифункциональности и полиаспектности графических знаков / Т.О.Анохина // Вестник Сумского гос. ун-та. Сер.: Филологические науки. – Сумы: СумГУ, 2014. - №3 (62). – С.9-14.
2. Искакова А.Ш. Языковое манипулирование через графон в рекламных текстах /А.Ш.Искакова, Б.С.Каболова, А.С.Сатанова. [Электронный ресурс]. – Режим доступа: http://rusnauka.com.
3. Куликова М.Н. соотношении понятий «графические стилистические средства» «фонографические средства» и «фонографическая стилизация» / Н.М.Куликова // Вестник СпбГУ. Сер.9, 2010. – Вып. 2. – с. 125-127.
4. Сковородников А.П. Экспрессивные синтаксические конструкции современного русского языка / А.П.Сковородников. – Томск. – 2011. – 255 с.

КОДИРОВАНИЕ ИНФОРМАЦИИ ПРОДУКЦИИ

Бачурина Вероника Игоревна, Мищенко Елена Алексеевна, студентка 2-го курса
Научный руководитель Иванова Анастасия Игоревна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Тенденцией нескольких последних десятилетий во многих странах, в том числе и в России, является внедрение разновидности информационных технологий, основанных на использовании штрихового кодирования (не только в торговле, сфере услуг, но и в промышленном производстве для идентификации печатных плат, сборочных узлов, изделий, упаковок, в почтовых и транспортных ведомствах, банковской системе, клиниках и пр.) по передаче информации с помощью носителя данных – символа штрихового кода.

Штриховым называют код, состоящий из знаков набора параллельных чередующихся темных (штрих) и светлых (пробел) полос различной ширины в соответствии с ГОСТ Р ИСО МЭК16022-2008. Размеры полос стандартизованы. Самый узкий штрих принят за единицу. Каждая цифра (разряд) складывается из двух штрихов и двух пробелов.

Технологии штрихового кодирования весьма эффективно применяют в розничной торговле, что имеет большое значение для потребителей. Наличие штрих-кода на товаре позволяет полностью автоматизировать процесс управления движения товаров от момента их поступления в магазин до продаж покупателю. Любые операции с каждой единицей товара учитываются в центральном компьютере магазина, тем самым обеспечивается автоматический контроль динамики продажи товара, изменение товарных запасов. Такая технология учета позволяет автоматизировать бухгалтерскую деятельность, анализировать итоги работы по структурным подразделениям, что заметно улучшает финансово-коммерческую деятельность торгующей организации, и оперативно удовлетворять нужды потребителей.

Информация в штриховом коде определяется соотношением ширины штрихов и пробелом. Высота не несет информационную нагрузку и выбирается из соображений легкости считывания – она должна обеспечить пересечение лучом сканера всех штрихов кода.

Штриховые коды можно условно разделить на два типа:

- товарные (имеют два ряда – штриховой и цифровой)
- технологические (имеют один ряд – штриховой).

Товарные кода были созданы специально для идентификации производимых товаров, учета их при транспортировке и управления складскими и торговыми процессами.

Штриховой ряд в товарном коде предназначен для оптического считывания путем поперечного сканирования. Сканер декодирует штрихи в цифры через декодер (микропроцессор) и вводит информацию о товаре в компьютер.

Цифровой ряд предназначен потребителю, информацию для которого ограничена только указанием страны и возможностью проверки подлинности штрих-кода по контрольному разряду. Полный штриховой код позволяет закупочным торговым организациям иметь четкие реквизиты происхождения товара и адресовано предъявлять претензии по качеству, безопасности и другим параметрам, не соответствующим контракту договора.

Разработано большое разнообразие товарных штрих-кодов. К ним относят код UPC, применяемый в США и Канаде, и код EAN, созданный в Европе на основе кода UPC и используемый практически на всех континентах.

Контроль штрих-кода необходим для исключения ошибок при вводе в компьютерные системы (особенно это качается кодов большой длины), а также для проверки подлинности штрих-кодов.

Алгоритм расчета контрольной цифры. Этот алгоритм применим для штрих-кодов EAN-8, EAN-13, UPC, ISBN, ISSN. При этом используется один и тот же алгоритм вычислений по модулю 10.

Для расчета контрольной цифры следует пронумеровать все разряды цифрового ряда справа налево, начиная с позиции контрольного разряда (первый).

Затем:

- начиная со второго, сложить цифры всех четных разрядов;
- полученную сумму умножить на 3;
- начиная с третьего, сложить цифры всех нечетных разрядов;
- сложить результаты, полученные во втором и третьем пунктах;
- значение контрольного разряда является наименьшим числом, которое в сумме с величиной, полученной в пункте 4 даст число, кратное 10.

Рассмотри пример вычисления контрольного разряда на примере любого штрих-кода.

Счетчик воды.

Произведем вычисление контрольного разряда для данного штрих-кода:

33918904

1) 3+1+9+4=17

2) 17×3=51

3) 3+9+8+0=20

4) 51+20=71

5) 71+9=80

Трубы пластиковые канализационные.

Произведем вычисление контрольного разряда для данного штрих-кода:

4028076183201

1)0+8+7+1+3+0=19

2) 19×3=57

3) 4+2+0+6+8+2=22

4)57+22=79

5)79+1=80

Полное совпадение контрольной цифры с добавляемой для кратности цифрой (1), следовательно, товар произведен законно и его качество гарантируется. Страна производитель Германия.

Произвести расчет и проверку законности мы можем абсолютно любой товар и продукцию.

В данной статье мы рассмотрели методику разработки, нанесения, считывания и расшифровки штрих-кодов. Система автоматизированной идентификации товара на много облегчит труд работников занимающимся учетом и продаж товаров, так как нанесение штрихового кода ускоряет процесс идентификации товара.

В условиях конкурентной среды значительная часть информации должна быть оперативной, а также недоступной для ее использования специально нерегламентированными пользователями. Такую возможность нам дает штриховое кодирование. Именно поэтому в последнее время штриховое кодирование стало играть большую роль не только в специфических сферах, но и в нашей повседневной жизни.

Список использованных источников

1. Хрусталёва, З.А. Метрология, стандартизация и сертификация. Практикум/ З.А. Хрусталёва. – М.: КНОРУС, 2017. – 280 с.
2. Штриховое кодирование // Студопедия. URL: https://studopedia.ru/13_172995_shtrihovoe-kodirovanie.html (дата обращения: 28.03.2021).

ОСОБЕННОСТИ ПОДГОТОВКИ КОНВЕРТЕРНЫХ ШЛАМОВ К РЕЦИКЛИНГУ

Беляев Никита Николаевич, студент 3-го курса
Суханов Павел Дмитриевич, студент 3-го курса
Научный руководитель: Казарцев Владимир Олегович., преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В настоящее время, несмотря на стремительное расширение областей применения неметаллических и композиционных материалов сталь по объемам производства, комплексу физико-механических и эксплуатационных свойств по-прежнему занимает лидирующие позиции среди известных конструкционных материалов. В структуре сталеплавильного производства ведущая роль традиционно принадлежит кислородно-конвертерному процессу

Выплавка стали в кислородных конвертерах является наиболее распространенным и прогрессивным способом ее производства. Это связано с высокой производительностью агрегатов, относительной простотой их конструкции, высоким уровнем автоматизации процессов, гибкостью технологии плавки, позволяющей в сочетании с внеагрегатной обработкой и непрерывной разливкой получать сталь высокого качества и широкого сортамента. Технология плавки стали в конвертере является важным звеном производственного процесса и определяет его основные технико-экономические показатели. Она состоит из совокупности различных операций, приемов и методов, выполняемых в определенной последовательности и сочетании для получения жидкого металла высокого качества. Классический кислородно-конвертерный процесс представляет собой выплавку стали из жидкого чугуна с добавкой лома в конвертере с основной футеровкой и продувкой кислородом сверху через водоохлаждаемую фурму

При конвертировании металла в зависимости от состава металлошихты, конструкции агрегата и технологии плавки образуется до 12 – 25 кг/т стали мелкодисперсной пыли, степень очистки отходящих газов от пыли превышает 80 %, степень утилизации составляет 72 % [1, 2]. Весьма ценным железосодержащим техногенным сырьем являются получаемые конвертерные шламы, в частности конвертерные шламы которые содержат до 57 – 65 % железа. Основная часть шламов представлена оксидом Fe_2O_3 [3, 4].

Рециклинг шламов в производственный цикл решает одновременно ряд важных задач: обеспечивает предприятия железосодержащим сырьем, решает экологические проблемы утилизации мелкодисперсных отходов [5, 6], способствует экономии природного сырья и снижению себестоимости производимой стали [4, 6, 7]. В связи с этим применение эффективных технологий рециклинга является одной из актуальных задач современной металлургии. При всей очевидной перспективности переработки конвертерных шламов существует и ряд проблем.

В частности, ввод железосодержащих материалов в доменную печь или конвертер осуществляется, как правило, в кусковом виде, в связи с этим техногенное сырье (прокатную окалину, пыль, обезвоженные шламы и т.п.) традиционно утилизируют посредством добавки в аглошихту [1]. Однако введение мелкодисперсных материалов в аглошихту в значительных количествах, как правило, сопровождается снижением производительности аглоустановок и ведет к ухудшению прочностных характеристик готового агломерата [3].

Не менее важным фактором, ограничивающим применение конвертерных шламов в качестве компонента шихты доменной плавки, является наличие в них оксидов цинка, отрицательно влияющих на стойкость корпуса и футеровки доменной печи.

Необходимо отметить, что экономическая и экологическая эффективность переработки отходов в металлургии возрастает при замене природных ресурсов отходами на более поздних стадиях металлургического передела [3]. В условиях решения проблемы рециклинга конвертерных шламов разработан и совершенствуется способ кондиционирования отходов высокой влажности, который включает их нетермическое адсорбционное обезвоживание и последующее термохимическое окускование [7]. Принципиальная схема разработанной технологии рециклинга конвертерных шламов представлена на рис. 1.

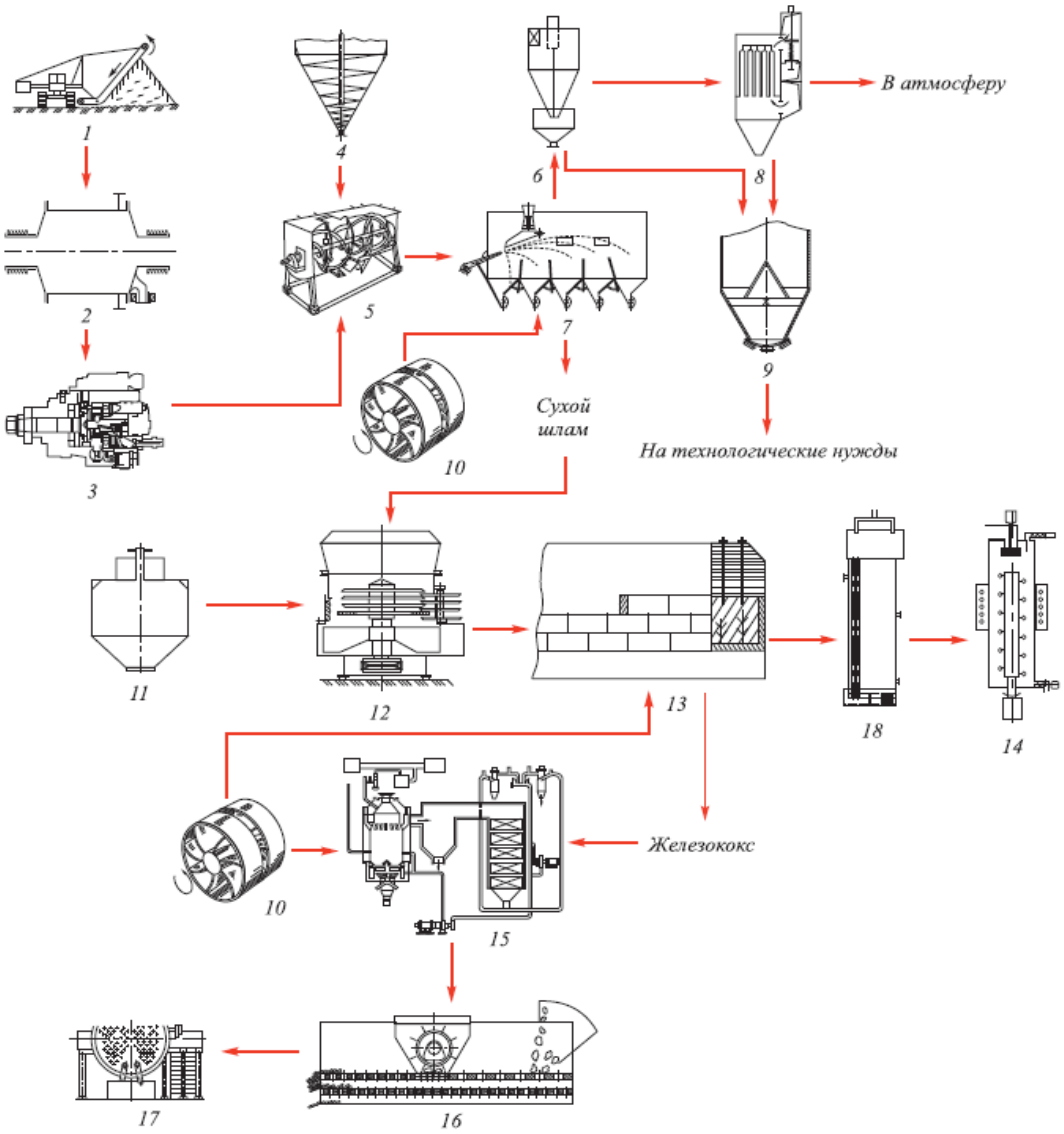


Рисунок 1 - Принципиальная схема процесса кондиционирования влажного конвертерного шлама адсорбционным обезвоживанием и термохимическим окускованием: 1 – шламонакопитель; 2 – сгуститель; 3 – шламовый насос; 4 – бункер БПК; 5 – смеситель-адсорбер; 6 – циклон; 7 – пневмоклассификатор; 8 – рукавный фильтр; 9 – бункер влажного БПК; 10 – воздуходувка; 11 – бункер угля ГЖ + Ж; 12 – смеситель; 13 – коксовая печь с вращающимся подом; 14 – газотурбинная установка (ГУБТ); 15 – установка сухого тушения кокса; 16 – сортировка железококса; 17 – котел-утилизатор; 18 – конденсатор

Конвертерный шлам (КШ) из шламонакопителя 1 поступает в сгуститель 2 и затем передается в смеситель-адсорбер 5 для контакта с мелкозернистым буро-угольным полукоксом (БПК), выполняющим функцию адсорбента влаги. Затем смесь БПК и КШ передается на разделение в пневмоклассификационную установку 7, откуда более легкий БПК через пылеотделительную систему (циклон 6, рукавный фильтр 8) поступает в бункер 9, откуда забирается на энерготехнологические нужды. Очищенный от пыли воздух сбрасывается в атмосферу. Более тяжелый шлам из пневмоклассификатора через дозирующее устройство поступает в смеситель 12, туда же из бункера 11 через дозирующее устройство поступает коксующийся уголь. В печи с вращающимся подом 13 полученная в заданном соотношении смесь подвергается термоокислительному коксованию. Полученный при конечной температуре 1100 – 1150 °С феррококс охлаждается в установке сухого тушения кокса (УСТК) 15, сортируется на классы 0 – 10 мм, 25 – 10 мм и +25 мм и поступает в котел-утилизатор 17. При сжигании над слоем шихты выделяющихся газообразных продуктов в печи с вращающимся подом выделяется тепло, которое используется для коксования. Одновременно на конечной стадии коксования при температуре 1050 – 1100 °С завершаются процессы восстановления оксидов железа до $Fe_{мет}$ и оксидов цинка до $Zn_{мет}$. Температура начала восстановления оксида цинка составляет 1070 °С. Продукты сгорания совместно с парами цинка из печи поступают в конденсатор 18, в котором пары цинка конденсируются и собирается жидкий металлический цинк. Оставшиеся газообразные продукты поступают в газотурбинную установку (ГУБТ) 14 для последующего применения.

В части рециклинга железосодержащих дисперсных отходов альтернативой агломерации могут быть процессы их окускования или брикетирования.

Широкие возможности для утилизации мелкодисперсных отходов обеспечивает брикетирование, оно перспективно и с точки зрения получения металлизованного продукта, так как в состав брикетируемой шихты могут быть введены восстановители. Преимуществом брикетов по сравнению с восстановленными окатышами является более низкое значение открытой пористости, вследствие чего брикеты не подвержены активному вторичному окислению на атмосферном воздухе [3].

Брикетирование является менее затратным способом утилизации отходов по сравнению с агломерацией или получением обожженных окатышей. Процессы брикетирования мелкодисперсных отходов наиболее технологичны, чем другие способы окускования, так как качество брикетов в наименьшей степени зависит от гранулометрического состава и влажности исходного материала, а их размер, форма и химический состав могут регулироваться в широких пределах путем подбора размера и формы ячеек матрицы, выбора связующих веществ и ввода различных добавок [3].

Также одним из основных преимуществ брикетирования состоит в том, что этот способ позволяет из отходов различного химического состава и свойств получить кондиционные продукты с регулируемыми размерами и технологическими свойствами, увеличить плотность сыпучих материалов, предотвратить зависание и слеживаемость мелкодисперсных отходов в бункерах и дозирующем оборудовании, снизить пыление в процессах транспортировки и использования [3].

Эффективность использования полезных компонентов в составе брикетов значительно выше, чем в каком-либо другом состоянии (в мелкой или полидисперсной фракции, в сортированном виде). По сравнению с агломерацией брикетирование железосодержащих отходов имеет целый ряд преимуществ [3]:

– брикеты имеют одинаковую форму и массу, характеризуются высокими содержанием железа, плотностью и прочностью, лучшей транспортабельностью;

– количество оборотного продукта на аглофабриках может достигать 20 – 25 % и более от общего потока шихты, в то время как на брикетной фабрике всего 2 – 6 %;

– весь кислород в брикете остается активным, в то время как в агломерате он находится в связанном состоянии (в виде силикатов), что особенно важно для доменного производства;

– экологическая безопасность брикетирования: безотходность, отсутствие высоких температур при изготовлении;

– возможность применения в брикете в любом соотношении углеродсодержащего наполнителя для активизации процессов в металлургической печи (карбюризатор, восстановитель, энергоноситель);

– возможность утилизации всех видов тонкодисперсных отходов металлургического производства.

Список использованных источников

1.Утилизация пыли и шламов в черной металлургии / А.И. Толочко, В.И. Славин, Ю.М. Супрун, Р.М. Хайрутдинов. – М.: Металлургия, 1990. – 206 с.

2. Su F., Lampinen H.-O., Robinson R. Recycling of Sludge and Dust to the BOF Converter by Cold Bonded Pelletizing // ISIJ International. 2004. Vol. 44. P. 770 – 776.

3. Металлургические технологии переработки техногенных месторождений, промышленных и бытовых отходов / С.Н. Кузнецов, Е.П. Волынкина, Е.В. Протопопов, В.Н. Зоря. – Новосибирск: Издательство СО РАН, 2014. – 294 с.

4. Переработка и утилизация промышленных отходов Челябинской области / И.П. Добровольский, И.Я. Чернявский, А.Н. Абызов, Ю.Е. Козлов. – Челябинск: Изд-во ЧелГУ, 2000. – 256 с.

5. Гостенин В.А., Елисеев Ю.П., Коваленкова Е.Ю., Неверовская И.П. Исследование возможности переработки шламов с целью получения железного концентрата // Сталь. 2016. № 4. С. 75, 76.

6. Комплексное использование сырья и отходов / Б.М. Равич, В.П. Окладников, В.Н. Лыгач, М.А. Менковский. – М.: Химия, 1988. – 288 с.

7. Вторичные материальные ресурсы черной металлургии / В.Г. Барышников, А.М. Горелов, Г.И. Папков и др. В 2-х т. Т. 2. – М.: Экономика, 1986. 344 с.

ИССЛЕДОВАНИЕ МЕХАНИЗМОВ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЙ НА ОСНОВЕ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Береговенко Владимир Олегович, магистрант кафедры теории и организации управления

Федеральное государственное бюджетное образовательное учреждение высшего образования «Гжельский государственный университет»,
Московская область

Создание оптимальной и эффективной системы государственного управления с целью решения неотложных социально-экономических проблем призвано создать условия для повышения уровня и качества жизни населения. Учитывая важнейшую роль промышленных предприятий и организаций в экономике государства, необходимым аспектом устойчивого развития видится повышение эффективности их деятельности. Вопросам государственного регулирования экономики посвящено значительное количество научных исследований. Проблемы необходимости и целесообразности государственного вмешательства в экономические процессы предлагается решать, применяя различные формы и методы государственного управления. Ряд исследований, посвященных этой проблеме, предлагает различные механизмы решения, основанные на цифровой трансформации государственного управления.

В исследовании эффективности деятельности государственных органов управления А.М.Нагимовой предполагается, что реформа государственного управления в России будет успешной, если на уровне каждого субъекта будет четкое понимание не только поставленных и решаемых целей и задач, проводимых мероприятий, но и будет внедрен механизм оценки достижения ожидаемых конечных результатов на основе использования цифровых технологий. При этом, социально-экономическое развитие региона зависит не столько от подотчетности региональных органов государственного управления населению, сколько от повышения эффективности деятельности органов государственного управления. [1]

Возрастающая актуальность исследований, направленных на формирование методологии стратегического управления конкурентоспособностью промышленных предприятий с целью повышения экономической эффективности их деятельности, в том числе за счет цифровой трансформации внутрихозяйственных резервов, рассмотрена в исследовании Е.В.Быковской. Предполагается, что развитие промышленных предприятий и организаций требует структурной, в том числе, и цифровой трансформации для обеспечения технологического прорыва и повышения конкурентоспособности экономики. Этот аспект предопределяет необходимость развития методологии управления их технологической конкурентоспособностью на основе изыскания внутренних резервов. [2]

Вопрос информатизации органов государственной и муниципальной власти рассмотрен в исследовании Г.С.Джура, как один из приоритетных в организации государственного управления. Учитывая тот факт, что сегодня информационные технологии являются ключевым фактором повышения эффективности деятельности, позволяя перейти на качественно новый уровень реализации всех функций государственного управления, таких как контроль, сбор и анализ информации, организация системы информационно – аналитического обеспечения выработки, принятия, реализации и оценки эффективности управленческих решений. При этом, важным направлением автоматизации этих процессов является создание единых информационных потоков и баз данных для всех уровней и ветвей государственной власти. [3].

Необходимость ускорения процессов цифровизации и цифровой трансформации государственного управления экономикой в целях достижения конкурентоспособности представлена в исследовании Ю.И.Грибанова с позиции аналитической и научно-методической проработки осуществления изменений. Ввиду того, что цифровая экономика

задает вектор развития социально-экономических систем на долгосрочную перспективу, требуется проведение исследований и всестороннего анализа самих процессов цифровой трансформации государственного управления. Пока механизмы ее осуществления остаются недостаточно изученными, что обуславливает потребность в развитии инструментария ее выявления и оценки управления. [4]

В докладе, подготовленном коллективом Центра технологий государственного управления Института прикладных экономических исследований Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации рассмотрены теоретические и практические подходы к цифровой трансформации государственного управления, прежде всего, в интересах обеспечения и повышения его результативности. Авторы оценивают влияние цифровизации на качество государственного управления и рассматривают аспекты результативности государственного управления на основе анализа зарубежного и отечественного опыта использования цифровых технологий при планировании, мониторинге и оценке результатов в государственном управлении. На современном этапе развития цифровые технологии позволяют преодолеть отдельные проблемы, а цифровая трансформация может стать драйвером для внедрения новой модели государственного управления – государственного управления по результатам. [5]

Анализируя опыт представленных исследований, можно сделать вывод о том, что вопросы цифровой трансформации государственного управления находятся на этапе внедрения отдельных механизмов, причем подходы к их использованию различны. Конечной целью каждого исследования видится результат – повышение эффективности деятельности. Однако, вопросы повышения эффективности деятельности промышленных предприятий и организаций на основе внедрения цифровой трансформации государственного управления являются недостаточно изученными. В этой связи, предлагается сначала исследовать отдельные механизмы повышения эффективности деятельности предприятий, затем, рассмотреть уровень внедрения в них государственного управления, а затем, предложить варианты его цифровой трансформации.

Список использованных источников

1. Нагимова А. М. Эффективность деятельности государственных органов управления
как фактор повышения качества жизни в регионе: проблемы оценки и измерения. – Казань: Казан. гос. ун-т, 2009. – 188 с.
2. Быковская Е.В. Стратегическое управление технологической конкурентоспособностью промышленного предприятия на основе мобилизации внутрихозяйственных резервов. – Курск: Юго-Западный гос.ун-т, 2019, 301с.
3. Государственное управление инновациями: проблемы, технологии, перспективы: сб. материалов II международной науч.-практ. конф., – Донецк: ДонНТУ, 2016. – 271 с.
4. Грибанов Ю.И. Цифровая трансформация социально-экономических систем на основе развития института сервисной интеграции URL: https://unecon.ru/sites/default/files/dissgribanovui.pdf
5. Добролюбова, Е. И., Южаков, В. Н., Ефремов, А. А., Клочкова, Е. Н., Талапина, Э. В., Старцев, Я. Ю. Цифровое будущее государственного управления по результатам М.: Издательский дом «Дело» РАНХиГС, 2019 - 114с.— (Научные доклады: государственное управление).

ВЫБОР УСТРОЙСТВ ДЛЯ ПОРЕЗКИ ПРОКАТА

Беседин Роман Викторович, студент 3-го курса
Научный руководитель Плохих Елена Вадимовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Вспомогательное оборудование прокатного стана делится на транспортное и обрабатывающее. К обрабатывающему можно отнести оборудование для порезки металла: ножницы и пилы. Выбор устройств для порезки должен быть обусловлен типом стана и технико-экономическими показателями работы цеха, поэтому эта тема является актуальной в настоящее время.

Цель исследования: проанализировать устройства для порезки металла (в частности, пилы), их преимущества и недостатки, выбрать наиболее подходящие устройства для порезки сортового проката

В зависимости от конструкции диска пилы разделяют на две группы: пилы для горячей и холодной резки.

Для горячей резки проката применяют диски с зубьями, которые снимают стружку и удаляют ее при вращении диска.

Дисковые пилы применяются для горячей и холодной резки сортового проката сложной формы поперечного сечения, а также крупносортного проката

По конструкции диски пил бывают с зубьями и в виде гладкого тонкого диска.

При использовании гладких дисков разрезание металла осуществляется за счет его разогрева и расплавления быстро вращающимся диском.

Диск обильно охлаждается водой или эмульсией (например, давление составляет до 30 бар и расход до 80л/мин. при порезке горячего металла в сортопрокатном цехе №1 АО ОЭМК).

Предельная скорость вращения диска ограничивается прочностью его материала;

Допустимое напряжение материала диска - 160 МПа;

Производительность пилы при горячем резании стали достигает 5000мм^2/с;

Подача диска пилы горячей резки (50...300) мм/с;

Подача диска пилы холодной резки до 1 м/мин.;

Стойкость диска при порезке стали марки ШХ-15 - 100мм

Параметры дисковых пил (диаметр, толщина, ход диска, максимальные размеры проката) регламентированы ГОСТ 5379.

Материал диска – сталь марки 45 или 65Г (для горячей резки и пил холодной резки с твердосплавными зубьями). Для пил холодной резки без наплавки зубьев применяются режущие диски из закаленной стали марки 9ХФ.

Пилы для холодной резки имеют гладкие диски или диски с мелкими зубьями. Работа этих пил основана на сильном повышении температуры на небольшом участке контакта, благодаря трению быстро вращающегося диска о металл. Поэтому такие пилы называются пилами трения. Расплавившиеся в месте реза частицы металла выбрасываются из прорези вращающимся тонким диском. Пилы трения обладают меньшей производительностью, и их применяют только в том случае, если по технологическим условиям прокат нельзя резать в горячем состоянии.

У пил холодной резки со стальным диском нижний предел окружной скорости диска составляет 40-50 м/сек. При таких скоростях диск может работать без охлаждения.

Верхний предел скорости диска, определяемый условиями прочности и наличием вибрации не превышает 120 м/сек.

При горячей резки окружная скорость диска находится в пределах 70-120 м/сек при интенсивном охлаждении водой высокого давления до 25-30 атм.

В заключение можно сказать, что выбор наиболее подходящих устройств для порезки сортового проката зависит от типа стана и технико-экономических показателей работы стана.

Список использованных источников

1. Колокольцев В.М. Основы металлургического производства. Учебник. М : Лань СПб, 2017. – 616 с.
2. Константинов И.Л. Основы технологических процессов обработки металлов давлением. Учебник. Красноярск: СФУ, 2015. – 488 с.
3. Рудской А.И. Теория и технология прокатного производства. Учебное пособие. С.-Пб. : «Наука», 2005. – 542 с.

ВЫБОР СПОСОБОВ ПРОИЗВОДСТВА МЕТАЛЛИЧЕСКИХ ТРУБ

Бородкин Максим Вячеславович, студент 3-го курса
Научный руководитель Плохих Елена Вадимовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Качество продукции является одним из важнейших факторов деятельности АО ОЭМК, в него входят не только понятие качества металла (стабильность в процессе эксплуатации металла заданных физических, химических и технологических свойств), но и требования к форморазмерам, состоянию поверхности, внутреннему строению металлопродукции, ее товарному виду, упаковке, маркировке, те показатели, которые отражаются в стандартах и подлежат обязательному выполнению.

Сортамент прокатного стана- это совокупность профилеразмеров и марок стали готового проката, производство которых обеспечивается техническими характеристиками и технологическими процессами на данном прокатном стане.

Сортамент профилей проката разнообразен. Профили круглого, квадратного, шестигранного и прямоугольного сечения составляют группу сортовых профилей общего назначения.

Потребители заказывают на металлургическом предприятии не вообще профиль проката, а профиль из определенной марки стали с показателями качества, нормируемыми определенными ГОСТ и ТУ.

Таблица 1 – Фасонные профили

Вид проката	ГОСТ, ОСТ, ТУ	Размеры, мм	Исходная заготовка
Общего назначения			
Сталь угловая: равнополочная	ГОСТ 8509-86	(20х20)...(250х250)	Заготовка
Балка двутавровая	ГОСТ 8239-72	№10..№70 (100...700)х(55...180)	Блюм, заготовка
Швеллер	ГОСТ 8240-72	№5...№40 (50...400)х(32...115)	-
Балки с параллельными полками	ГОСТ 26020-83	высота 200...1000	-
Отраслевого назначения			
Рель железнодорожный колеи типа Р 75... Р 43	ГОСТ 16210-77 и др.	-	Блюм, заготовка
Железнодорожные скрепления	ГОСТ 8194-75 и др.	-	Заготовка
Специального назначения			
Сталь горячекатанная, рессорнопружинная	ГОСТ 7419.1-78 и др.	Круг и квадрат размером до 80мм; полоса (5...18)х(20...150)	Заготовка
Сталь прокатанная для напильников	ГОСТ 5210-82	11 профилей	Заготовка

Таблица 2 – Периодические профили

Вид проката	ГОСТ, ОСТ, ТУ	Размеры, мм	Исходная заготовка
Сталь горячекатанная для армирования железобетонных конструкций	ГОСТ 5781-82	№6...№80	Заготовка
Профиль для лемехов, для автомобильной промышленности	ГОСТ 8531-78 и др.	20 профилей	–

Таблица 3 – Специальные виды проката

Вид проката	ГОСТ, ОСТ, ТУ	Размеры, мм	Исходная заготовка
Колесо цельнокатанное	ГОСТ 9036-76	Наружный диаметр 950...1050	Слиток
Бандаж для колес ЖД вагонов, локомотивов, трамвая	ГОСТ 3225-80	7 профилей	Заготовка
Шар для мельниц	ГОСТ 7524-83	Диаметр 20...200	–
Коленчатые валы, оси переменного сечения, шестерни, втулки и др.	По ТУ машиностроительных предприятий	–	–

Из трубной заготовки, выпускаемой на ОЭМК, производят бесшовные трубы, которые широко востребованы во всем мире. По характеру использования трубы делят на трубы для различных трубопроводов, трубы для бурения, эксплуатации скважин, для машиностроения. Цель исследования: проанализировать сортамент стана и способы производства металлических труб.

Трубы по конструкции делят на гладкие (трубы для трубопроводов машиностроения) и нарезные (все трубы для бурения и эксплуатации скважин и часть труб для трубопроводов).

Все стальные трубы в зависимости от метода изготовления делят на три основные группы: бесшовные горячекатаные (ГОСТ 8732), электросварные (ГОСТ 10704) и холоднодеформированные (ГОСТ 8734).

Задачи исследования: рассмотреть сортамент стана для производства трубной заготовки; рассмотреть способы производства металлических труб; провести анализ доступной информации; выбрать наиболее перспективный способ производства металлических труб.

Сортопрокатный цех № 1 ОЭМК производит трубную заготовку диаметром от 90 до 190 мм, длиной от 4500 до 5900мм и от 9000 до 11800 мм (по ГОСТ 2590)

Марочный сортамент стана для внутреннего рынка включает широкий спектр марок сталей для производства трубной заготовки: стали нефтяного сортамента: марок 30Г2 ,32Г2, 32Г2С, 36Е2С, 37Г2С, 30ХМА, для производства обсадных, бурильных, насосно-компрессорных труб классов прочности Д, К, Е (по ГОСТ 4543); котельные стали марок 20, 12Х1МФ, 15ГС для изготовления паропроводных труб энергоблоков с высокими и сверхкритическими параметрами пара (ГОСТ 1050, 4543, 20072); стали для труб, имеющих повышенную стойкость против сероводородной коррозии: марки 12ГФ, 16ГФБ, 28ГМ и т.д. (по ГОСТ 4543).

Предусмотрена поставка проката на экспорт по зарубежным стандартам ASTM, DIN. Сортовой прокат и трубная заготовка из нелегированных марок стали: С20, С30, С40, С43, СК45, ST 37.3, 070М20, SAE 1018, SAE1045, и из легированных марок стали, включая хромомолибденоникеливые марки: 16 MnCr5, 42CrMo4, 40NiCrMo4, 48MnV3,3MnSi5, SAE 9262.

Трубная заготовка, производимая СПЦ-1 ОЭМК используется для производства бесшовных труб.

Сопоставление сортамента позволяет сделать следующие выводы:

1) сортамент сварных труб по диаметру значительно шире, чем сортамент бесшовных труб (8–1620 и 25–550 мм соответственно);
2) сварные трубы могут быть изготовлены со значительно меньшим отношением толщины стенки к диаметру (до 0,005) по сравнению с бесшовными трубами (0,04–0,05);
3) минимальная толщина стенки сварных труб значительно меньше, чем бесшовных (1 и 2,5 мм соответственно);
4) максимальная толщина стенки бесшовных труб значительно больше, чем сварных (16 и 75 мм соответственно).

Трубы холоднодеформированные имеют значительно меньшие размеры: диаметр до 4 мм и толщину стенки до 0,2 мм. Их получают из горячекатаных и сварных труб. Трубы изготавливают из нелегированных, легированных, коррозионностойких, подшипниковых сталей. Сортамент сталей, из которых получают бесшовные трубы, намного шире, чем сортамент сталей, из которых изготовляют сварные трубы.

Наиболее распространенными трубопрокатными агрегатами являются агрегаты с автоматическим, пилигримовым, непрерывным и трехвалковым раскатным станом.

Для массового производства тонкостенных труб проводится продольная прокатка труб на длинной оправке в нескольких последовательно установленных двухвалковых клетях (непрерывная прокатка). На них обычно прокатывают трубы диаметром 57–114 мм.

Для получения толстостенных труб из слитков диаметром 168–550 мм на пилигримовых станах осуществляется цикл деформации гильзы в трубу за каждый оборот валка с переменным радиусом калибра. При этом направление вращения валков противоположно направлению истечения металла и за каждый цикл подвергается деформации небольшая часть гильзы.

Трехвалковые станы косой прокатки предназначены для получения толстостенных труб высокой точности диаметром 60–180 мм, для производства подшипниковых труб.

Для уменьшения диаметра труб, полученных после раскатных станов, применяют продольную прокатку без оправки в редукционных станах, которые состоят из ряда последовательно установленных двух-, трех- или четырехвалковых клетей, когда прокатку ведут с натяжением, что позволяет изменить диаметр трубы и толщину стенки. На редукционных станах обычно прокатывают трубы диаметром 25–76 мм.

Таблица 4 – Распределение коэффициентов деформации на трубопрокатных агрегатах

Тип стана	Коэффициент вытяжки при прошивке	Коэффициент вытяжки при раскатке
Автоматический	1,3-5,2	1,2-2,1
Непрерывный	1,3-2,5	3,0-6,5
Пилигримовый	1,3-2,1	3,0-15,0
Трехвалковый	1,3-2,1	1,8-3,2
Реечный	1,3-2,1	7,0-20,0

Производительность, т/ч, любого трубопрокатного стана:

$$A=3600\ M\ k_и/((T_м+T_в)\ a),$$

где M – масса слитка или заготовки, т;

kи – коэффициент использования стана;

Тм – машинное время прокатки одной штуки, с;

Тв – время вспомогательных неперекрывающихся операций, с;

а – коэффициент расхода металла.

Машинное время определяют эмпирически. Время вспомогательных операций определяют хронометражем или расчетом скорости перемещения вспомогательных механизмов и построением графика операций. Коэффициент использования стана принимают равным 0,9–0,97. Коэффициент расхода металла определяют расчетом или принимают по статистическим данным. Машинное время прошивки:

$$T_{пр} = (L_р + L_г)/(v_{пр}\ \eta_0 \sin \varphi),$$

где $L_р + L_г$ – путь, проходимый передним торцом заготовки-гильзы, м;

$L_р$ – длина используемой части бочки валка, м;

$v_{пр}$ – окружная скорость валков, м/с;

η_0 – коэффициент осевого скольжения;

φ – угол подачи.

В заключение можно сказать, что каждый из способов имеет определенные технологические преимущества, недостатки и в зависимости от технико-экономических показателей работы стана, выбирается оптимальный вариант.

Список использованных источников

4. Колокольцев В.М. Основы металлургического производства. Учебник. М : Лань СПб, 2017. – 616 с.
5. Константинов И.Л. Основы технологических процессов обработки металлов давлением. Учебник. Красноярск: СФУ, 2015. – 488 с.
6. Рудской А.И. Теория и технология прокатного производства. Учебное пособие. С.-Пб. : «Наука», 2005. – 542 с.

ВЫБОР МАТЕРИАЛА И СПОСОБА ИЗГОТОВЛЕНИЯ ПРОКАТНЫХ ВАЛКОВ

Колодич Виталий Ростиславович, студент 3-го курса
Научный руководитель Плохих Елена Вадимовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Актуальность: основным рабочим инструментом каждой прокатной клети являются валки и от качества валков напрямую зависит качество производимого проката и производительность цеха.

Цель исследования: проанализировать материалы и способы изготовления прокатных валков, выбрать наиболее перспективный способ.

Задачи: - рассмотреть способы изготовления прокатных валков;

- изучить материал валков;
- провести анализ доступной информации;
- предложить наиболее эффективный способ изготовления прокатных валков.

Объект исследования: рабочие валки прокатной клети.

Валки прокатных станов осуществляют пластическую деформацию обрабатываемого металла, придают ему необходимую форму и размеры поперечного сечения. В процессе деформации вращающиеся валки воспринимают давление обрабатываемого металла, возникающее в очаге деформации и передают его опорным валкам, валковым подшипникам, нажимному устройству, станине рабочей клети.

Рабочие валки должны обеспечивать надежный, устойчивый (без пробуксовки) захват металла, обладать необходимой механической прочностью при воздействии на них изгибающих и скручивают усилий (от моментов сил, действующих в очаге деформации), иметь достаточную твердость износоустойчивость рабочей (контактной) поверхности, подвергающейся термоциклическому нагружению при прокатке.

Для изготовления валков прокатных станов применяются сталь и чугун.

Сталь для изготовления валков используется литая, кованая, углеродистая, качественная конструкционная и легированная. В отдельных случаях, валки подвергаются термической обработке (закалке или нормализации с отпуском). Литые валки изготавливают путем заливки жидкой стали в вертикально установленные литейные формы или методом центробежного литья. Валки куются или прессуются из стальных слитков. Масса слитка: (1,0…200,0) т. и более. Уков слитка (поперечная деформация) должен быть в пределах 2,5…3,0, чтобы при ковке была плотность разрушена хрупкая литая структура металла.

Стальные валки изготавливаются по следующим стандартам:

- ГОСТ 9487-70 (технические требования к валкам)
- ГОСТ 5399-69 (основные размеры валков);
- ГОСТ 3541-74 «Стальные кованые валки для станов холодной прокатки»
- Межзаводские технические условия – для валков стана горячей прокатки.

Чугун для изготовления валков используемся только литой. Чугунные валки используются на клетях трио, в качестве рабочих валков чистовых клетей сортовых станов. В настоящие время чугунные валки составляют серьезную конкуренцию стальным валкам.

Формы для отливки валков располагаются строго вертикально. Применяется и центробежная отливка чугунных валков.

Если чугун залить в тонкостенную металлическую форму (кокиль), то поверхность отливки быстро охладится (закалится). Структура закаленных (отбеленных) объемов отливки будет состоять из твердого, но хрупкого цементита (Fe_3C), что характерно для структуры белого чугуна. По такой технологии отливают только бочкой балков, а остальные части валка отливаются в утепленные формы. Валки с отбеленной бочки имеют высокую износостойкость, а шейки и треф хорошо сопротивляются скручиванию.

С целью дальнейшего повышения эксплуатационной надежности чугунных валков прокатных станов применяется технология изготовления, так называемых, двухслойных легированных валков.

Вначале в вертикально установленную форму для отливки валка заливают чугун, легированный, как правило, хромом и никелем. После застывания поверхностного слоя бочки в кокиле, в эту же форму заливают нелегированный чугун обычного химического состава, вытесняющий (промывающий) еще не застывшие объемы легированного чугуна. Таким образом из легированного, закаленного чугуна формируются только поверхностные слои бочки валка глубиной отбела до 50 мм, что обеспечивает их износостойкость, механическую прочность и твердость. В поперечном сечении бочки чугунного валка (в изломе бочке) должны быть всегда ясно различимы невооруженным глазом три слоя: поверхностный белый, переходной (равномерно серо-белый, без местных скоплений цементита и графита) и внутренний центральный – из серого чугуна.

Валки сортовых станов могут отливаться с калибрами, которые затем растачиваются на станках для получения точных размеров, требуемых технологией прокатки.

Влияние отдельных химических элементов на качество и эксплуатационную надежность чугунных валков:

- увеличение содержания кремния в чугуне уменьшает толщину отбеленного слоя на поверхности бочки валка;
- повышение содержания марганца в чугуне уменьшает прочность валка из-за увеличения глубины отбела и толщины переходного (бело-серого) слоя в структуре материала валка;
- сера и фосфор приводят к увеличению хрупкости валка;
- молибден повышает прочность и износостойкость валка;
- магний, в небольших количествах, улучшает структуру чугуна и повышает прочность валка; магниевый чугун конкурирует с литой сталью при применении его в черновых клетях станов;
- медь, при содержании в чугуне до 2,5%, уменьшает количество карбидов в чугуне. При этом твердость поверхности валка не снижается, а термостойкость и износоустойчивость, в среднем возрастают на 30%;
- хром и никель значительно повышают прочность и износостойкость валков.

Следует отметить, что чугунные валки в 2…2,5 раза дешевле стальных. Учитывая их большую износостойкость, эксплуатационные расходы при применении чугунных валков сокращаются в 5…6 раз, в сравнении со стальными.

Применяются в прокатном производстве и составные валки. Валки большой массы (например, опорные валки листовых станов) целесообразно изготавливают составными: на стальную ось, хорошо работающую на изгиб, нагорячо или прессовой посадкой одевается сменный износостойкий стальной бандаж.

Твердосплавные валки применяется в чистовых блоках современных высокоскоростных проволочных станов. Валки (в виде дисков) изготавливаются из твердого сплава типа карбида вольфрама. Износостойкость таких валков в 30…50 раз выше, чем у стальных, легированных валков. Из этого же материала изготавливают рабочие валки двадцативалковых станов для холодной прокатки узких полос и лент толщиною до 0,05 мм из высокопрочных прецезионных сплавов.

Для обработки поверхности калибров твердосплавных валков (бандажей) применяются специальные металлорежущие станки.

Калибры валков блочных клетей (чистовых блоков проволочных станов, а также блоков для горячей калибровки проката, установленных в технологических потоках мелкосортных и среднесортных станов) могут обрабатываться непосредственно в станине блока (без разработки блока для извлечения валков).

Таким образом, чугунные валки в 2…2,5 раза дешевле стальных и имеют большую износостойкость, эксплуатационные расходы в сравнении со стальными. Также в чистовых блоках современных высокоскоростных проволочных станов применяется твердосплавные валки из твердого сплава типа карбида вольфрама.

Список использованных источников

7. Колокольцев В.М. Основы металлургического производства. Учебник. М : Лань СПб, 2017. – 616 с.
8. Константинов И.Л. Основы технологических процессов обработки металлов давлением. Учебник. Красноярск: СФУ, 2015. – 488 с.
9. Рудской А.И. Теория и технология прокатного производства. Учебное пособие. С.-Пб. : «Наука», 2005. – 542 с.

ФАКТОРЫ, ВЛИЯЮЩИЕ НА ОКИСЛЕНИЕ И ОБЕЗУГЛЕРОЖИВАНИЕ МЕТАЛЛА

Логвинова Людмила Алексеевна, студентка 4-го курса
Научные руководители: Гугнина Алла Викторовна, преподаватель
Плохих Елена Вадимовна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Актуальность: Процессу нагрева металла перед обработкой всегда сопутствуют такие явления, как окисление и обезуглероживание. Важно уметь регулировать окисленный и обезуглероженный слой металла.

Цель исследования: проанализировать факторы, влияющие на окисление и обезуглероживание металла

Задачи:

- рассмотреть процесс окисления металла;
- рассмотреть процесс обезуглероживания металла;
- провести анализ доступной информации;
- рассмотреть факторы, позволяющие регулировать окисленный и обезуглероженный слой металла.

Объект исследования: нагрев металла перед обработкой.

Обезуглероживание – уменьшение концентрации углерода в сталях и сплавах, возникающее при нагреве в окислительных средах, а также в водороде. Обезуглероживание стали и сплавов может оказывать как вредное, так и полезное действие. Обезуглероживание стали, происходящее при термической обработке, нагреве под прокатку или ковку, распространяется на большую или меньшую глубину внутрь металла и приводит к ухудшению свойств поверхности готовой продукции и браку.

Окисление металла представляет собой процесс взаимодействия окисляющих газов, с железом и легирующими элементами. Этот процесс зависит не только от химических реакций окисления, но и от закономерностей образования окисной пленки. По мере ее роста она все больше и больше изолирует сталь от газов.

Поэтому скорость роста окалины зависит не только от протекания химического процесса окисления стали, но и от условий передвижения ионов металла (от металла и внутренних слоев окалины к внешнему) и атомов кислорода (с поверхности металла к его внутренних слоев), т.е. от условий протекания физического процесса двусторонней диффузии.

1. Влияние факторов на окисление

На пути от заготовки до готового изделия металл обычно несколько раз нагревается в различных печах. При высоких температурах его поверхность окисляется, и часть металла переходит в окалину. Уменьшение массы металла в результате окисления, выраженное в килограммах или процентах, называется угаром. В камерных и методических нагревательных печах нормальным считается угар стали 1–2%. Приблизительно можно считать, что около 5% общей выработки стали переходит в окалину при нагреве в различных печах. Потери стали вследствие угара составляют не меньшую величину, чем потери от коррозии.

По мере повышения температуры стали скорость окисления увеличивается и наиболее интенсивно процесс протекает при температуре выше 1000° С. Сталь образует три окисла: FeO – вюстит (температура плавления 1377° С); Fe203 — гематит (температура плавления 1538° С); Fe304 – магнетит (температура плавления 1565° С). Окалина представляет собой смесь всех трех окислов, но ее средний состав приближается к Fe304.

Процесс окисления представляет собой двустороннюю диффузию, при которой кислород диффундирует извне к внутренним слоям стали, а железо – изнутри к наружным

слоям окалины. На окисление влияет ряд факторов, основные из которых температура, время нагрева, состав печной атмосферы и химический состав стали. Чем выше температура стали, тем интенсивнее окисление; чем быстрее идет процесс нагрева, тем оно меньше. Окислению препятствует образование окалины на поверхности металла.

2. Влияние факторов на обезуглероживание

Одновременно с окислением железа происходит окисление углерода поверхностного слоя стали – обезуглероживание. Если скорость окисления больше скорости обезуглероживания, то обезуглероженного слоя не образуется. При большей скорости обезуглероживания под слоем окалины обнаруживается обезуглероженный слой.

Обезуглероживание вызывает изменение механических свойств. Сталь с обезуглероженной поверхностью характеризуется малой сопротивляемостью против статических нагрузок, низким пределом усталости и склонностью к короблению. Наиболее подвержены обезуглероживанию стали со значительным содержанием углерода, например, инструментальные, шарикоподшипниковые и др.

В результате обезуглероживания образуется газообразный продукт, который диффундирует в обратном направлении. Наиболее обезуглероживающей средой служит водяной пар, затем водород, кислород и, наконец, двуокись углерода. Скорость диффузии зависит от разности концентраций диффундирующих веществ и константы диффузии, зависящей от температуры. С повышением температуры и содержания углерода глубина обезуглероживания увеличивается.

Обезуглероживание стали зависит от времени выдержки при высокой температуре, коэффициента избытка воздуха, сорта сжигаемого топлива, температуры, состава стали, степени обжатия металла при обработке давлением. Минимальное обезуглероживание для большинства углеродистых сталей получается в том случае, когда в продуктах сгорания содержится 1-3% свободного кислорода. С этой точки зрения нагрев высокоуглеродистых и быстрорежущих сталей в печах безокислительного нагрева нежелателен, так как в печной атмосфере присутствуют в большом количестве водород и водяной пар. Решающее влияние на глубину обезуглероживания прокатного или тянутого металла оказывает степень обжатия. Чем больше обжатие и увеличение удельной поверхности изделия, тем меньше глубина обезуглероживания конечного продукта прокатки. Из легирующих элементов обезуглероживанию способствуют алюминий, кобальт и вольфрам; хром и марганец задерживают обезуглероживание. Кремний, никель и ванадий не оказывают существенного влияния на обезуглероживание. Наиболее эффективными способами уменьшения обезуглероживания в настоящее время являются: при нагреве стали перед прокаткой — скоростной нагрев в пламенных печах, а при нагреве до 1000–1100° С - в муфельных и электрических печах с контролируемой атмосферой. В последнее время исследуется нагрев сталей в расплавленном стекле. Этот очень перспективный метод позволит защитить металл от окисления и обезуглероживания почти полностью.

Таким образом, очень перспективным методом защиты металла от окисления и обезуглероживания, является нагрев в муфельных и электрических печах с контролируемой атмосферой, а также нагрев сталей в расплавленном стекле.

Список использованных источников

10. Колокольцев В.М. Основы металлургического производства. Учебник. М : Лань СПб, 2017. – 616 с.
11. Константинов И.Л. Основы технологических процессов обработки металлов давлением. Учебник. Красноярск: СФУ, 2015. – 488 с.
12. Рудской А.И. Теория и технология прокатного производства. Учебное пособие. С.-Пб. : «Наука», 2005. – 542 с.

ИССЛЕДОВАНИЕ ТЕХНОЛОГИЙ СКЛАДИРОВАНИЯ МЕТАЛЛА, ИСПОЛЬЗУЕМЫХ В СОРТОПРОКАТНОМ ЦЕХЕ №1

Масалов Никита Витальевич, студент 4-го курса
Научный руководитель Береговенко Елена Николаевна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Сортопрокатный цех №1 (СПЦ-1) Оскольского электрометаллургического комбината (ОЭМК) выпускает крупносортный прокат простой формы сечения: круглый диаметром от 80 до 190мм; квадратный со стороной от 70 до 130мм; подкат для стана 350 сечением 170 х 170мм; подкат для шаропрокатного стана диаметром 100 и 120мм. [1]

Исходным полупродуктом для производства проката в СПЦ-1 служит непрерывно-литая заготовка, поступающая из электросталеплавильного цеха. Традиционно, участки цеха располагаются в соответствии с оптимальным перемещением грузопотоков по стадиям технологического процесса от исходной заготовки до получения готового проката. При этом, складские помещения цеха имеют ряд существенных отличий, позволяющих не только обеспечить хранение сырья и готовой продукции, но и оптимизировать работу отдельных участков.

Цель исследования состояла в выявлении аспектов оптимизации производственного процесса посредством использования эффективных технологий складирования металла.

Объектом исследования был выбран Оскольский электрометаллургический комбинат.

Предметом исследования – технологический процесс производства проката в СПЦ-1.

Рассмотрим общее назначение и технологию складирования металла в сортопрокатном цехе №1 Оскольского электрометаллургического комбината.

Склад литой заготовки располагается на начальном этапе технологического процесса. Его задача состоит в обеспечении 5-7 суточного запаса сырья – непрерывно-литой заготовки (НЛЗ) сечением 300 х 360мм. Технологией предусмотрено, что они передаются из отделения адъюстажа электросталеплавильного цеха на склад литой заготовки, где их поплавочно укладывают в ячейки. Перемещение заготовок осуществляется магнитными кранами. Заклейменные торцы складированных НЛЗ должны быть направлены в одну сторону. Допускается складировать НЛЗ заклейменными торцами в противоположную сторону, если это установлено технической документацией на производство конкретных видов продукции. НЛЗ складируют в ячейки не более чем в семь рядов. Для НЛЗ с порезом от 4.2 до 4.6м и от 8.0 до 9.2м допускается складировать заготовки в восемь или девять рядов. НЛЗ, предназначенные для отгрузки потребителю, складируют поплавочно в ячейках или на двух стеллажах, расположенных в 1 и 3 пролетах СЛЗ вдоль железнодорожных путей. [2]

Высотный промежуточный склад располагается между пролетами участков стана и отделения отделки, завершая линию расположения оборудования участка охлаждения и термообработки. Технологией предусмотрена загрузка проката штабелерами в один из трех пролетов склада. При загрузке проката управление штабелерами производится в автоматическом режиме. Место складирования каждого пакета автоматически определяет система PR-Z, в соответствии с состоянием склада на данный момент, и передает координаты места складирования, номер пакета и массу пакета в систему управления PR-L. В случае невозможности работы высотного штабелера в автоматическом режиме управление работой штабелера производит оператор поста управления в полуавтоматическом режиме. Оператор вводит с пульта управления координаты свободного места, после чего штабелер подходит к заданному месту и складирует пакет. После складирования пакета система PR-L передает данные загруженного пакета в систему PR-Z, которая обеспечивает слежение за металлом, отображение состояния склада, выдачу данных по запросу, ввод и корректировку

данных, протоколирование. Учет принимаемого на склад проката производят в АСУП СПЦ-1 по общей массе плавки и количеству прутков в плавке. После загрузки плавки на склад оператор вводит в систему PR-L номер загруженной плавки и сводит баланс плавки в соответствии с заданием на прокатку. [3]

Склад готовой продукции (СГП) предназначен для размещения готового проката по партиям и заказам для отгрузки потребителю. Передачу проката на СГП с участков отделки и механизированного стеллажа производят в соответствии с суточным графиком отделки и отгрузки проката. Складирование пакетов проката на СГП производят в штабели поплавочно. Пакеты проката одной единицы заказа складируют не более чем в двух местах складирования. Пакеты проката в штабеле должны быть уложены ровно, рядами крест на крест, без перекоса в рядах. Не допускается в штабеле укладывать пакеты проката на крайние обвязками других пакетов. Торцы пакетов с клеймом в штабеле должны быть направлены в одну сторону. Высота штабеля должна быть не более 4,0 м. Расстояние между штабелями должно быть не менее 1,0 м. Расстояние от ближайшего железнодорожного рельса до штабеля должно быть не менее 20 м при высоте штабеля не более 1,2 м и не менее 2,5 м при высоте штабеля более 1,2 м. Расстояние от выступающих частей передаточной тележки до штабеля должно быть не менее 1,0 м После начала складирования на СГП новой плавки сортировщик-сдатчик проверяет правильность места складирования плавки. После окончания складирования каждой плавки сортировщик-сдатчик СГП распечатывает приемо-сдаточную накладную на принимаемую плавку и проверяет прокат. В приемо-сдаточной накладной указана попакетная информация проката (номер плавки, номер партии (единицы заказа), марка стали, вид и размер профиля, длина, номер заказа позиции, номера пакетов, масса пакетов, количество прутков в пакетах, время поступления каждого пакета на шлеппер (передаточную тележку), место складирования, общая масса и общее количество прутков). При проверке складированного проката сортировщик-сдатчик СГП проверяет маркировку, нумерацию пакетов, целостность упаковки и соответствие количества складированных пакетов проката данным приемо-сдаточной накладной. На принятых на СГП пакетах экспортного проката, окружаемых автотранспортом, допускаются дополнительные проволочные обвязки в четыре скрученные между собой в двух местах. [4]

Рассмотрев виды и технологии складирования металла в условиях СПЦ-1, можно отметить, что расположение склада литой заготовки и склада готовой продукции является традиционным. Применение технологии промежуточного складирования металла позволяет обеспечить автономную и бесперебойную работу участков стана и отделения отделки, что положительным образом сказывается на увеличении производительности как отдельных участков, так и всего сортопрокатного цеха.

Список использованных источников

6. Основные производства ОЭМК им. А.А. Угарова // Металлоинвест. Металлургический сегмент. URL: https://www.metalloinvest.com. (дата обращения: 28.03.2021).
7. Приемка, складирование и отгрузка непрерывнолитой заготовки на складе литой заготовки СПЦ-1. ТИ П.03 – 46 – 2010, г.Старый Оскол, типография АО «ОЭМК», 2010, 10с.
8. Приемка, складирование и выдача проката на промежуточном высотном складе СПЦ-1. ТИ П.03 – 215 – 2010, г.Старый Оскол, типография АО «ОЭМК», 2010, 7с.
9. Приемка, складирование и отгрузка проката на складе готовой продукции СПЦ-1. ТИ П.03 – 156 – 2009, г.Старый Оскол, типография АО «ОЭМК», 2009, 12с.

КОНСТРУКТИВНЫЕ ОСОБЕННОСТИ ВАЛКОВ ШАРОПРОКАТНОГО СТАНА

Махортов Андрей Романович, студент 4-го курса
Научный руководитель Береговенко Елена Николаевна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Производство проката в условиях Оскольского электрометаллургического комбината (ОЭМК) завершает полный металлургический цикл предприятия и обеспечивает более широкие возможности для реализации металлопродукции. Сортопрокатный цех №1 выпускает крупносортный прокат; сортопрокатный цех №2 и цех отделки проката выпускают среднесортный и мелкосортный прокат; шаропрокатный стан обеспечивает выпуск шаров крупного диаметра. [1]

Основным рабочим инструментом каждого прокатного стана являются прокатные валки. Их устанавливают в прокатной клети, формируя рабочие пары для совместной работы. В одну пару, как правило, подбирают валки с одинаковыми характеристиками для обеспечения равномерности деформации металла. Каждый валок состоит из бочки (контактирующей с металлом в процессе обработки), шеек (опор валка) и концевой (приводной) части. Конструкции валков зависят от назначения стана и вида выпускаемой металлопродукции. [2]

В связи с вводом в эксплуатацию нового шаропрокатного стана (ШПС), на котором, в отличие от продольной прокатки сортопрокатного производства используется поперечно-винтовая прокатка, цель исследования состояла в выявлении конструктивных особенностей применяемых прокатных валков.

Объектом исследования был выбран Оскольский электрометаллургический комбинат.

Предметом исследования – технологическое оборудование шаропрокатного стана.

Шаропрокатные станы предназначены для производства методом горячей винтовой прокатки в винтовых калибрах стальных шаров, используемых преимущественно в качестве мелющих тел для шаровых мельниц в горнорудной, угольной и других отраслях промышленности, а также, в качестве заготовок шаров для подшипников качения и шаровых заготовок различных машиностроительных деталей. Шары производства ШПС предполагается использовать на мельницах горно-обогатительных комбинатов, входящих в состав УК Металлоинвест: Михайловского и Лебединского.

Производство шаров методом прокатки в настоящее время приобретает все большую популярность. Это объясняется тем, что прокатные изделия по качеству превосходят изделия, изготовленные другими способами. При прокатке волокна металла не разрываются, а приобретают форму изделия, тем самым увеличивая его прочностные характеристики. Главные преимущества процесса прокатки шаров по сравнению с ковкой и штамповкой:

- прокатные шары имеют более правильную форму и более точные размеры;
- производительность при прокатке шаров в 3-8 раз больше, чем при ковке и штамповке;
- стойкость валков прокатных станов в несколько раз превышает стойкость штампов;
- непрерывность процесса прокатки позволяет механизировать и автоматизировать производство шаров. [3]

Основной рабочий инструмент стана для прокатки шаров – прокатный валок с винтовым калибром. По характеру деформации калибр валка условно можно разделить на две части: формирующий участок, на котором осуществляется захват заготовки и ее постепенное обжатие в шар, соединенный перемычкой с остальной частью заготовки и отделочный участок, где производится калибровка шара и отделение его от основной заготовки. Формовка шаровой заготовки производится ребордами, высота которых

постепенно возрастает. Для упрощения расчета калибровки и изготовления валков принято, что высота реборд калибра изменяется по закону прямой линии.

Исходным параметром для конструирования валка является его размер по вершинам реборд. Диаметр валка выбирают по следующим условиям: надежный захват металла валками; прочность валка; отсутствие налипания металла на валок; наименьшая стоимость и минимальный износ валков.

Для обеспечения нормального процесса прокатки профиль и размеры формующего участка калибра рассчитываются таким образом, чтобы в процессе обжатия заготовки соблюдались следующие три основных условия:

1. Объем металла, обжимаемый в калибре, должен оставаться постоянным в течение всего процесса формовки шара.
2. Изменение профиля и размеров реборды калибра должно соответствовать вытяжке обжимаемой заготовки.
3. Обжатие должно осуществляться относительно узкими участками, чтобы предотвратить разрушение металла в осевой зоне заготовки.

Таким образом, реборда на различных участках калибра должна иметь строго определенную толщину. В связи с этим, формующий участок калибра имеет переменный шаг нарезки. Отделочный участок калибра имеет постоянный шаг и профиль, соответствующий профилю прокатываемого шара.

Эти конструктивные особенности прокатных валков шаропрокатного стана, при правильном ведении процесса, обеспечат получение изделий, по симметрии и качеству поверхности, по структуре и механическим свойствам, удовлетворяющих требованиям, предъявляемым к шарам.

Список использованных источников

10. Основные производства ОЭМК им. А.А. Угарова // Металлоинвест. Металлургический сегмент. URL: https://www.metalloinvest.com. (дата обращения: 28.03.2021).
11. Береговенко Е.Н. Обработка металлов давлением: учебное пособие. г.Старый Оскол, типография СТИ НИТУ «МИСиС», 2014, 134 с.
12. Производство шаров на шаропрокатных станах // ЭЗТМ. URL: https://www.eztm.ru. (дата обращения: 28.03.2021).

ПЕРЕРАБОТКА ЦИНКОСОДЕРЖАЩЕЙ ПЫЛИ

Самофалов Ярослав Николаевич и Серова Снежана Александровна,
студенты 4-го курса
Научный руководитель Плохих Елена Вадимовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Актуальность: Вопрос рационального использования техногенного сырья с применением современных технологий важен, т.к. металлургические предприятия стремятся к максимальному снижению воздействия производства на окружающую среду.

Цель исследования: проанализировать способы переработки пыли металлургических цехов в условиях НЛМК, выбрать наиболее перспективный способ.

Задачи:

- - рассмотреть способы переработки пыли;
- - провести анализ доступной информации;
- - предложить наиболее эффективный способ переработки цинкосодержащей пыли.

Объект исследования: отходы металлургических предприятий.

Железосодержащее техногенное сырье на НЛМК представлено шлаками, шламами, пылями, окалиной, хвостами. Пыль образуется в газоочистных установках. Конвертерная пыль на Новолипецком металлургическом комбинате образуется в количестве около 10 тыс. т. и из-за высокого содержания цинка не может быть вовлечена во внутренний рециклинг. Пыль электродуговых печей производств НЛМК-Калуга и НЛМК-Урал при образовании около 40 тыс. т. частично продается, а частично утилизируется сторонними предприятиями.

Для решения поставленных задач был использован кейс- метод.

Главной проблемой мы выявили недостаточную эффективность схемы обращения с техногенным сырьем. Причины образования этой проблемы можно разделить на 3 вида:

- экономическая - высокая стоимость переработки и падение спроса на часть продукции;
- технологическая - увеличение объема отходов, непригодных к устранению и сложность вовлечения отходов в производство;
- экологическая - негативное влияние захоронений на окружающую среду и увеличение площади захоронения отходов.

По диаграмме Исикавы мы выявили основную цель – повышение эффективности схемы обращения с техногенным сырьем. Для достижения данной цели были представлены следующие задачи:

1. Выделение цинка из пыли газоотчисток;

2. Установка системы ScanDust; сбор пыли в фильтрах газоотчистки и сбор оксида цинка.

По технологии SMART цель включает в себя 5 пунктов:

1. Конкретная: найти применение пыли с высоким содержанием цинка;

2. Измеримая: уменьшение отходов производства на 3%;

3.Достижимая: данная система показала свою эффективность на других производствах;

4. Актуальная: данная система способствует увеличению эффективности утилизации техногенного сырья;

5. Ограниченная во времени: в течении 5 лет.

Были рассмотрены четыре системы: «Separate Filter», VHR-процесс, «ScanDust», «Брикетирование», способствующие достижению поставленной цели и с помощью метода ранжирования была найдена более результативная система – ScanDust. К данному выводу мы пришли в ходе анализа 4-х факторов (экономичность, реализуемость, экологичность и эффективность).

Так же мы провели SWOT-анализ. Сильной стороной системы ScanDust является выделение цинка из улавливаемой пыли. Слабой стороной - необходимость в монтаже оборудования над каждым источником пыли. Возможностью является вовлечь полученный цинк в процесс производства оцинкованного проката. Угрозой является простой оборудования и сложности в транспортировке.

Принцип работы системы ScanDust.

ScanDust является примером плазменного способа переборки железо содержащих отходов. Пыль электросталеплавильного процесса поступает в смеситель с коксом, водой и перемешивается. Лишняя вода удаляется, а смесь инжектируется в нижнюю часть плазменного генератора. Конечные продукты - металл, шлак и газ. Металл возвращают в металлургический цикл, шлак можно использовать для дорожно-строительных работ, газ можно возвращать в плазменный генератор или использовать для теплоснабжения. Уловленный цинк отделяют и восстанавливают в других процессах.

На подготовку к внедрению нам понадобится 8 мероприятий, которые продлятся 22 месяца, затем внедрение 3 месяца, после этого будет выполнена оценка экономического и экологического эффекта, которые займут 2 и 3 года соответственно. Отчёт будет выполнен по результатам экономического эффекта.

Экономический анализ показал: коэффициент эффективности инвестиций-7,15; прирост рыночной стоимости - 315 млн. тыс. руб., чистая терминальная прибыль - 5,9 млн. тыс. руб., индекс рентабельности инвестиций - 2,5.

На долю предприятий черной металлургии приходится 15-20% общих загрязнений атмосферы промышленностью, что составляет более 10,3 млн. т вредных веществ в год, а в районах расположения крупных металлургических комбинатов – до 50%. На НЛМК образуется около 300 тыс. т. пыли. Твердые отходы занимают полезные площади, а из-за ветров происходит постоянное пыление отвалов, что приводит к загрязнению воздушного бассейна. Осадки (дожди, снег) выщелачивают из отвалов элементы и соединения, что приводит к заражению почвы. В итоге, даже освобожденные из-под отвалов земли становятся непригодными для сельскохозяйственного использования, образуются так называемые «индустриальные пустыни».

Таким образом, если большую часть источников цинкосодержащей пыли обрабатывать с помощью системы ScanDust, то данное решение будет иметь как экологический, так и экономический положительный эффект для предприятия.

Список использованных источников

1. Befesa ScanDust. URL: https://scandust.se/ (дата обращения: 28.03.2021).
2. НЛМК. URL: https://nlmk.com/ru/about/documents/?apply_filter=Y&documents_filter%5Bkeywords%5D=&documents_filter%5Bsection%5D=all&documents_filter%5Byear%5D=all&documents_filter%5Bperiod%5D=&as_sfid=AAAAAAXMLGLNl2rohX-EldBV3jD1encCgurOW-nZ4j-OVYx6d7GW02ZWUJlWIqtokNpUJA4dkQcP_mUoyLCO7wY07FUB_PO0fR-5_fFmQiB5dWiDwqSMLItfdzsSQIUbDLgGnQU%3D&as_fid=28bc01177cbfeab173fcb66e583ff9e657021b3f (дата обращения: 28.03.2021).

Секция 1.2

АНАЛИЗ ВЛИЯНИЯ ПАНДЕМИИ КОРОНАВИРУСА НА МАЛЫЙ БИЗНЕС В РОССИЙСКОЙ ФЕДЕРАЦИИ

Арская Алина Сергеевна, студентка 2 курса
Кувашова Людмила Владимировна, студентка 3 курса
Научный руководитель Пихтерева Марина Алексеевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Исследованиями последствий пандемии covid – 19 ученые всего мира будут заниматься еще очень и очень долго. До конца не изучен сам вирус, появляются новые штаммы, за второй волной следует третья. Сам вирус и ограничительные меры, связанные с ним, оказали колоссальное влияние на жизнь людей во всем мире.

Наша работа посвящена, пожалуй, одному из самых пострадавших объектов экономики – малому предпринимательству. Последнее представляет собой один из важнейших секторов экономики, способствующих развитию конкурентной рыночной среды, наполнению потребительского рынка товарами и услугами, созданию новых рабочих мест, формированию широкого круга собственников, развитию малых форм производства, что свидетельствует об актуальности проблемы исследования.

Если говорить более конкретно, то нас интересовало, насколько сильным оказалось влияние пандемии на малый бизнес в нашей стране.

Принято считать, что история малого бизнеса в России (тогда еще в СССР) начинается в 1987 – 1988 гг., когда эта сфера деятельности начала расширяться, количество людей, принимающих в нем участие, увеличиваться, предпринимательство стало приобретать характер активного многочисленного движения [1].

Что же касается современной истории, то сегодня в экономической науке не существует единого подхода к определению «малого предпринимательства» [4]. А в отечественной литературе и вовсе данное понятие одновременно отождествляют с: сектором экономики, экономической категорией и хозяйственной системой [4].

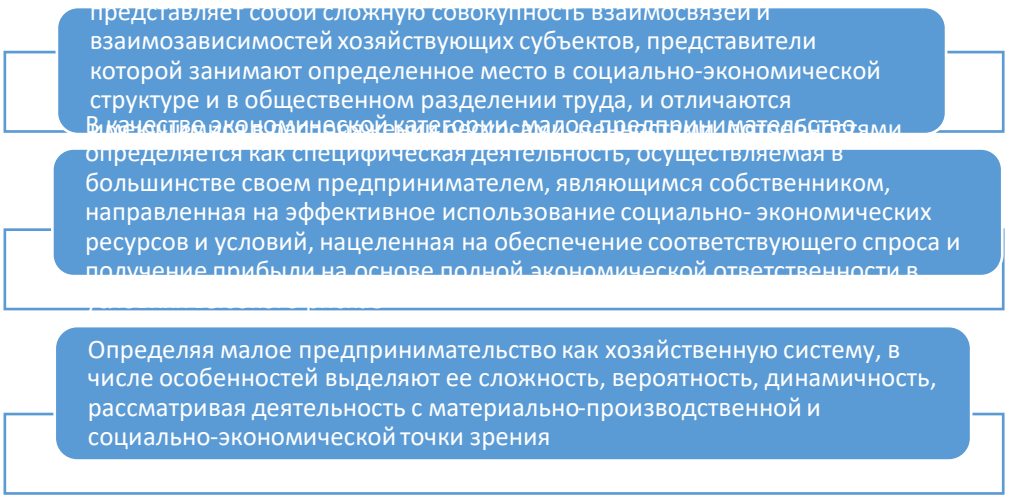


Рис. 1 – Подходы к определению «малое предпринимательство»

В действующем российском законодательстве конкретное определение малого предпринимательства не сформулировано, однако говорится о том, что это хозяйствующие

субъекты, к которым относят юридических лиц и индивидуальных предпринимателей, отвечающих ряду критериев, закрепленным в нормах Федерального закона «О развитии малого и среднего предпринимательства».

В работе также говорится о проблемах, которые существовали в среде малого предпринимательства до пандемии. По мнению, самих предпринимателей (опрос 2019 г от Альфа-банка) главные проблемы выглядят следующим образом [2]: снижение покупательского спроса, высокие налоги, недостаток кадров.

Если же говорить о мнении экспертного сообщества, то здесь отмечается острая конкуренция, несовершенство налоговой и законодательной базы, сложности кредитования, региональный аспект, административное давление.

На наш взгляд, пандемия covid – 19 лишь обнажила указанные проблемы, сделав их еще более острыми.

По данным апрельского замера Индекса RSBI – ежемесячного исследования бизнес-настроений малого и среднего бизнеса, организованного «Промсвязьбанком» (ПСБ) совместно с «Опорой России», после введения режима самоизоляции падение спроса отметили 80% предпринимателей сектора малого и среднего бизнеса [5]. То есть проблема спроса действительно стала еще насущнее.

В разрезе по размеру бизнеса наиболее пострадали микропредприятия – среди них падение спроса отметили 85% опрошенных. Малый и средний бизнес пострадал немного меньше: спрос упал у 74% и 76% соответственно[7].

Что касается видов деятельности, то здесь ожидаемо сильнее всех пострадали сферы услуг и торговли – сокращение спроса зафиксировали 82% и 81% предпринимателей соответственно. Промышленные предприятия отметили меньшее падение, спрос сократился у 73%[6,7].

Наконец, согласно первой оценке Росстата, ВВП страны упал по итогам 2020 года на 3,1%, а реальные доходы граждан уменьшились на 3,5%, безработица достигла 5,9 %. [3].

«Согласно исследованиям и статистике, прекратило работу 1,95 млн малых и средних предприятий, это почти каждый пятый в России. Общее число МСП сократилось более чем на 240 тыс., или на 4,2%, до 5,6 млн.», - сообщил член генерального совета «Деловой России» Алексей Мостовщиков [3].

Отметим также меры поддержки малого и среднего бизнеса в нашей стране государством в период пандемии [6]:

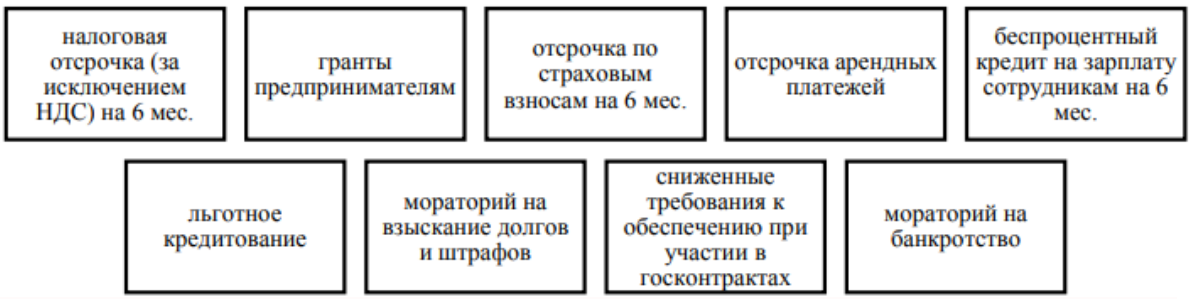


Рис. 2 – Меры поддержки малого и среднего бизнеса в РФ в период пандемии

Здесь стоит добавить, что к концу 2020 указанные мероприятия несколько смягчили удар коронавируса по малому бизнесу.

Так, по данным контрольно-кассовой техники, обороты по сектору МСП за полтора месяца 2021 года на 90% восстановились до уровня начала 2020 года [3].

Учитывая колоссальное падение спроса, падение реальных доходов граждан, рост безработицы, серьезные ограничительные меры с одной стороны, и помощь со стороны государства как для малых предприятий, так и для граждан, а также постепенный рост спроса к марту 2021 года, в заключении исследования делаются следующие выводы:

- нельзя забывать о пандемии, то есть ведение бизнеса должно быть с оглядкой на рекомендации властей, необходим постоянный мониторинг ситуации, знание, в данном случае, действительно сила;

- со стороны государства, на наш взгляд, требуется дополнительное стимулирование спроса населения, а также продолжение оказания поддержки малому бизнесу, поскольку эти два элемента тесно взаимосвязаны.

В заключении, на наш взгляд, можно сказать, что помимо целого ряда отрицательных моментов, пандемия в итоге приведет к снижению числа конкурентов на рынке (то есть останутся самые сильные и умелые), к появлению новых видов трудовой деятельности (например, дистанционный режим работы в прежние времена не пользовался популярностью), к накоплению опыта ведения бизнеса в подобных «шоковых условиях».

Таким образом, влияние covid – 19 нельзя охарактеризовать однозначно «кошмарным» для малого бизнеса в нашей стране, хотя негативных моментов действительно больше, однако после кризиса всегда идет подъем, надеемся, что он уже начался.

Список использованных источников

1. Батуро А.Ю. Проблемы и перспективы развития малого бизнеса в России// Научно – методический электронный журнал «Концепт». – 2017. – Т.39. – С.281 – 285

2. Волкова О., Малый бизнес назвал четыре главные проблемы. – [Электронный ресурс] - Режим доступа: https://www.top.rbc.ru/economics/25/09/2015/560574bf9a7947d1198f6d2

3.Доклад «Социально-экономическое положение России» – [Электронный ресурс]. – Режим доступа: https://rosstat.gov.ru/compendium/document/50801

4. Кремин А.Е. Теоретические подходы к определению категории малого предпринимательства //Экономика и социум. - 2015. - № 3-1 (16). - С. 959-967

5. Осведомлен – значит вооружен. Как будет развиваться нынешний кризис // [Электронный ресурс]. – Режим доступа: https://quote.rbc.ru/news/article/5e9464be9a7947a7d1a39918?utm_refen.yandex.com

6. Парламент принял новый пакет законов для поддержки граждан в условиях коронавируса. – [Электронный ресурс]. – Режим доступа: http://duma.gov.ru/news/48320/

7. 80% компаний МСП отметили снижение спроса с начала пандемии коронавируса – [Электронный ресурс]. – Режим доступа: https://www.psbank.ru/Bank/Press/News/2020/06/01-01

ВЕНТИЛЯЦИЯ ЖИЛОГО ДОМА

Афанасьев Александр Валериевич, студент 4-го курса
Научный руководитель Канайчева Ольга Васильевна,
преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Давайте представим, что вы тратите огромные деньги на изоляцию вашего дома, а Вам говорят, что в нем надо сделать отверстие, чтобы впустить холодный воздух. Или же представим ситуацию: что вы строите дом по новым энергоэффективным стандартам. А Вам говорят, что, чем больше вы в нем отверстия сделает, тем будет лучше. Да нас просят именно об этом, и все-таки почему?

Давайте разберемся!

Мы не можем контролировать стоимость отопления, но мы можем контролировать количество энергии необходимой для обогрева наших помещений. Чем меньше мы используем энергии для отопления, тем больше людей мы можем избавить от дефицита энергии и минимизировать воздействие на окружающую среду. Подобный подход к потреблению энергии с позиции здравого смысла и стимулирует повышение стандартов жилищного строительства и национальных программ по улучшению жилищного фонда.

В то время, как мы спешим утеплить свои дома, мы должны помнить, что мы должны в них жить, и жить в них так как никогда раньше. На самом деле до 90 % своего времени мы проводим в закрытых помещениях. Качество воздуха внутри может быть гораздо хуже, чем снаружи, что создает ряд проблем включая респираторные заболевания.

Таким образом мы стоим перед дилеммой перетягивания каната пытаемся закрыть наши дома чтобы сохранить тепло и открыть их чтобы впустить свежий воздух.

Вентиляция и является тем механизмом, с помощью которого мы выпускаем плохой воздух и впускаем свежий.

Что же такое плохой воздух?

В действительности причиной ему, мы и наша деятельность, за исключением таких вентиляции таких устройств, как камины и бройлеры, плохой воздух можно разбить на три основные группы:

1. Влажность, речь идет о приготовлении пищи, стирки, сушки и т.д. Семья из 4-х человек, производит до 16 литров влаги в сутки, если влажность не убирать она конденсируется на холодных поверхностях, далее образуется плесень, которая наносит ущерб нашему дому и также создает идеальную среду для размножения других гадостей. (Здорово если у Вас АСТМА!).
2. Метаболизм. Дело касается точно нас, в выделенном при дыхании CO2 содержится больше влаги и запахов. Запахи могут быть просто не приятными, но большое количество вдыхаемого CO2 воздействует на нас негативно, влияя на концентрацию внимания и усталость.
3. ЛОС – летучие-органические соединения. В общем это довольно, сложные химические вещества, присутствие которых вокруг нас нежелательно, большинство из них конечно не так уж плохи, но есть и очень вредные, например, красках и лаках и т. д.

Хорошая вентиляция поможет нам снизить риск их распространения.

Мы можем легко обнаружить такие загрязнители, как влажность, например, принимая душ. И проблемы которые они создают тоже довольно заметны, плесень, с другими загрязнителями может быть посложнее. Напоминает немного история с кипящей лягушкой, сейчас объясню: лягушка конечно сразу отреагирует на кипяток, но если ее поместить в холодную воду и медленно нагревать она будет сидеть там вполне счастливо пока ... конец известен.

Были ли вы когда-нибудь в спальне подростка, качество воздуха в ней сравнимо с прыжком в кипящую воду, сам обитатель еще спит и кажется хорошо себя чувствует. Словом, мы ведем себя безответственно, когда нам приходится признать, что качество воздуха внутри помещения плохое, особенно когда он накапливается вокруг нас медленно.

Поговорим о небольшом отверстии в стене, простой системе вентиляции. Мало вероятно, что мы прервёмся от просмотра передачи чтобы, слегка приоткрыть отверстие или закрыть его перед сном контролируя таким образом CO2. Почувствовав первое дуновение холодного воздуха, мы обычно закрываем отверстие и часто оставляем его в таком виде.

Загвоздка в том, что до сих пор нам это сходило с рук, потому что так много воздуха поступает через не плотности, но строя все более герметичные дома или утепляя старые, мы все больше полагаемся на вентиляцию. Вентиляционное отверстие закрыто или шумный вентилятор отключен, каким еще образом воздух будет еще попадать внутрь. Не ужели мы медленно превращаемся в лягушек.

Игнорируя установку или отказывая от интеграции соответствующей системе вентиляции в своих домах, мы подвергаем себя к недопустимому риску. Хотя отверстие в стене и имеет приделы, сегодня существует много отличных альтернатив. Правильная хорошо продуманная вентиляция обеспечивает хорошее качество воздуха внутри помещения и создает благоприятную и энергосберегающую среду проживания.

Список использованных источников

1. ГОСТ 34060-2017 «Инженерные сети зданий и сооружений внутренние. Испытание и наладка систем вентиляции и кондиционирования воздуха. Правила проведения и контроль выполнения работ».
2. Приказ Федерального агентства по техническому регулированию и метрологии от 16 января 2018 г. N 4-ст межгосударственный стандарт ГОСТ 34060-2017 введен в действие в качестве национального стандарта Российской Федерации с 1 февраля 2018 г.
3. Боровков В.С. Аэрогидродинамика систем вентиляции и кондиционирования воздуха / В.С. Боровков, Ф.Г. Майрановский.– М.: Стройиздат, 1978. - 120 с.
4. СНиП 41-01-2003 «Отопление, вентиляция и кондиционирование».
5. Стефанов Е.В. Вентиляция и кондиционирование воздуха. Инженерные системы зданий. – С-Пб : Издательство «Авок Северо-Запад», 2005. – 401 с.

ТРАГИЧЕСКИЕ СТРАНИЦЫ ИСТОРИИ ВЕЛИКОЙ ОТЕЧЕСТВЕННОЙ ВОЙНЫ: КОЛЛАБОРАЦИОНИЗМ

Болгов Егор Алексеевич, студент 1 курса
Шорстов Сергей Викторович, студент 1 курса
Научный руководитель Слободенюк Наталия Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Коллаборационизм (фр. collaboration - «сотрудничество») - осознанное, добровольное и умышленное сотрудничество с врагом, в его интересах и в ущерб своему государству. Первоначально коллаборационизм означал взаимодействие граждан Франции с немецкими властями в период Второй мировой войны. Позже это понятие стало применяться и к другим европейским правительствам, действовавшим под германской оккупацией.

В нашей стране термин «коллаборационизм» стал употребляться относительно недавно. В советской исторической науке обычно использовались слова «предатель», «изменник родины», «пособник». Взаимодействовать с оккупационным режимом приходилось очень многим советским людям, которые не решились вступить в ряды партизан. По подсчётам историков, около 10% населения тем или иным образом сотрудничали с оккупантами. Ведение сельскохозяйственной деятельности, ремонт дорог, уборка в административных учреждениях, преподавание в школах - все эти действия на территориях, захваченных немцами во время войны, попадают под определение коллаборационизма.

Так, например, в период оккупации города Старый Оскол с июля 1942 г. по февраль 1943 г. некоторые представители интеллигенции продолжали работать в открытых немцами учреждениях. Среди них: врачи С. Петрова и А. Кузнецова, агрономы Кротов и Мирошникова, учителя – Шестаков Ф.Л., Никонов, Васильев, Думченко Е., Рождественская В.М. и А. Алтухова. Историки-краеведы рассматривают их деятельность как приспособленчество и осуждают за проявление пассивного коллаборационизма [1].

Одной из наиболее трагичных тем в истории СССР является активный военный коллаборационизм. В военных подразделениях фашистской Германии во время Великой Отечественной войны служило более 1 млн. человек. Из местных жителей оккупированных территорий формировали вспомогательные полицейские части, которые позволяли немецкой администрации поддерживать порядок в населенных пунктах.

По воспоминаниям старооскольца Н.П. Коршикова, в городской полиции служили четверо бывших работников «Ремстройуправления». Они ходили по домам с белыми повязками на рукавах и собирали для немцев валенки, полушубки. Среди полицаев упоминаются братья Нестеренко, совершившие много злодеяний [6]. Есть также свидетельства о доносительстве среди населения Старооскольского района. Например, жертвами доносов односельчан стали колхозник П.С. Бороновский, семья коммуниста П.И. Чурикова. Городской голова Свешников выдал комсомолку Аню в руки следователя по политическим делам при немецкой комендатуре [1]. Также полицаи должны были отлавливать «окруженцев» - солдат Красной Армии, выбравшихся из котлов. В июле 1942 г. в селе Жуково Старооскольского района местный житель выдал полицаям нескольких красноармейцев. Бойцы были подвергнуты пыткам, а затем убиты [5].

Степень вины людей, которые в той или иной форме сотрудничали с оккупантами, была разной. Это признавало руководство советским Сопротивлением еще в начальный период войны. Среди старост и прочих представителей «новой русской администрации» были люди, занявшие эти посты по принуждению, по просьбам своих односельчан и по заданию советских спецслужб. Для немцев создавалась легенда об активном антисоветском прошлом этих людей, а на самом деле они саботировали распоряжения фашистов и

защищали местных жителей. Так, например, действовали Коновалов Я.И. и Горбань И. в селе Обуховка Старооскольского района Курской области.

Основную массу среди военных коллаборационистов составляли пленные. Именно в плену командир 2-й ударной армии Волховского фронта генерал-лейтенант А.А. Власов согласился на сотрудничество с руководством Третьего рейха, возглавив «Комитет освобождения народов России» (КОНР) и Русскую освободительную армию (РОА).

Гитлеровцы успешно вербовали представителей национальных меньшинств Советского Союза, пользуясь идеей создания независимых государств. Стратегия была эффективна там, где национальный вопрос был особенно острым - Украина, Прибалтика, Кавказ, Средняя Азия. Особое внимание уделялась казачьим отрядам, мечтавшим о независимости казачества.

Значимых успехов в сражениях против Красной Армии и войск антигитлеровской коалиции пособники нацизма не достигли. Те же формирования РОА мало напоминали армию и занимались в основном охраной и борьбой с партизанами. Но истории известно немало громких карательных операций, совершённых предателями против собственного народа: трагедия в Бабьем Яру, Крюковская трагедия и другие. В Старом Осколе особой жестокостью отличался начальник полиции по фамилии Лацун, загубивший около двухсот соотечественников. За службу нацистам он был награждён медалями и получил звание обер-лейтенанта [5].

В период оккупации расправу над пособниками фашистов вершили партизаны: в наградном листе командира-комиссара Старооскольского партизанского отряда Г.П. Кожедубова указано, что под его руководством было уничтожено 15 изменников родины. В связи с начавшимся освобождением Советской страны возникла необходимость в принятии специального законодательного акта для наказания тех, кто в годы оккупации творил злодеяния против советских граждан. Был издан указ Президиума Верховного Совета СССР от 19 апреля 1943 года «О мерах наказания для немецко-фашистских злодеев, виновных в убийствах и истязаниях советского гражданского населения и пленных красноармейцев, для шпионов, изменников Родины из числа советских граждан и для их пособников». Меры предусматривались самые строгие: злодеев, шпионов и изменников карали смертной казнью, пособников из местного населения ссылали на каторжные работы на 15-20 лет [4]. После освобождения Старого Оскола от войск противника в городе действовал истребительный батальон в количестве 220 человек, в задачи которого входили розыск и предание суду предателей.

Через 10 лет после окончания Великой Отечественной войны, 17 сентября 1955 года, был принят Указ Президиума Верховного Совета СССР «Об амнистии советских граждан, сотрудничавших с оккупантами в период Великой Отечественной войны 1941-1945 гг.». Согласно этому документу, амнистия применялась «...в отношении тех советских граждан, которые в период Великой Отечественной войны 1941-1945 гг. по малодушию или несознательности оказались вовлеченными в сотрудничество с оккупантами». Четвертая статья данного указа гласила, что амнистия не применяется «к карателям, осужденным за убийства и истязания советских граждан» [Цит. по 2, с. 11]. Так справедливое возмездие настигло начальника старооскольской полиции Лацуна, когда он, спустя много лет, вернулся из-за границы на родину. Вместе с другими предателями он был расстрелян по приговору суда [5].

Среди причин, которые приводили к коллаборационизму с гитлеровцами, историки обычно называют: недовольство советской властью (коллективизация и раскулачивание крестьянства, религиозная политика, массовые политические репрессии 1930-х гг.), личные амбиции, меркантильные интересы, ситуация безысходности, условия плена. Но всё же главную роль играли не политические, идейные мотивы сотрудничества с врагом, а обстоятельства вынужденного содействия с целью выживания в условиях немецкой оккупации. Таким образом, не любое сотрудничество с врагом можно квалифицировать как

измену или предательство. Если бы это было так, то пособниками гитлеровцев могли считаться все народы оккупированных стран, в том числе и 80 миллионов наших сограждан.

Коллаборационизм – явление многоликое, не до конца изученное. Историкам ещё предстоит дать всестороннюю объективную оценку одной из самых трагических страниц истории Великой Отечественной войны.

Список использованных источников

1. **Белых Н.Н. Частичка Родины (**Из истории Старооскольского края). URL:https://belstory.ru/goroda/stary-oskol/tchastitchka-rodin-18.html
2. Ковалёв Б.Н. Коллаборационизм в России в 1941-1945 гг.: типы и формы: НовГУ им. Ярослава Мудрого. – Великий Новгород. 2009. – 372 с. (Серия «Монография»; Вып. 10).
3. Коллаборационизм в годы Великой Отечественной войны. URL:https://mt-smi.mirtesen.ru/blog/43991102931/Kollaboratsionizm-v-godyi-Velikoy-Otechestvennoy-voynyi
4. **Семиряга В. Коллаборационисты.** URL:https://zavtra.ru/books/kollaboratcionisti
5. Теплов Ю. Возмездие через годы // Зори, № 30, 24 апреля 2020, С. 8
6. Чернов С. Бывшего начальника полиции судили в клубе мехзавода // Оскольские новости, № 5, 5 февраля 2002, С. 26

РЕАЛИЗАЦИЯ ГРУППОВОГО ПРОЕКТА «СПОСОБЫ ОЧИСТКИ ВОДЫ ОТ ОРГАНИЧЕСКИХ ЗАГРЯЗНИТЕЛЕЙ» ПРИ ИЗУЧЕНИИ ПРИКЛАДНОЙ ХИМИИ

Булинг Екатерина Сергеевна, студент 3-го курса
Научный руководитель Сутягин Андрей Александрович, заведующий кафедрой химии, экологии и методики обучения химии, доцент, кандидат химических наук
Южно-Уральский государственный гуманитарно-педагогический университет, г. Челябинск

Целью изучения дисциплины «Прикладная химия», реализуемой на выпускном курсе студентов, обучающихся по направлению Педагогическое образование (профильная направленность Биология. Химия), является знакомство с основными направлениями использования достижений химической науки в хозяйственной деятельности человека. Одним из важнейших объектов данной деятельности выступает вода, как природный ресурс, без участия которой невозможна реализация ни одного из направлений жизни человека. Возрастающий уровень водопотребления приводит к усилению негативного воздействия, оказываемого человеком на водные системы, что требует поиска путей рационального водопользования, а также разработки и реализации эффективных технологий восстановления водного ресурса. В связи с этим, знакомство с методами очистки воды является важнейшим вопросом, включенным в содержание материала, изучаемого в области прикладной химии.

Одной из эффективных форм учебной и исследовательской работы, реализуемых в современной школе, является проектная деятельность, направленная на развитие личностных качеств обучающихся через решение конкретной проблемы с достижением конкретного запланированного результата. В связи с этим, развитие у будущих учителей умений осуществлять проектную деятельность выступает в качестве обязательного образовательного компонента педагогического вуза, как одно из важнейших средств формирования личностных качеств студентов, определяющих его готовность к педагогической деятельности [1]. Кроме того, технология проектного обучения выступает как инструмент создания условий для развития креативных способностей и качеств личности студента, что является необходимым качеством в дальнейшей творческой деятельности педагога. Следует отметить, что проектные работы обучающихся, связанные с исследованием водных объектов, приобрели большую популярность, что связано с личностной заинтересованностью ученика, понимающего практическую важность воды в жизни каждого человека [8].

Распространенной формой проектной работы является выполнение группового проекта, направленного на осуществление небольшим коллективом общей идеи, при котором каждая мини-группа решает свою «узкую» задачу, а объединение результатов приводит к достижению одной общей цели. В связи с этим, в рамках выполнения курсовой работы нами разработан вариант группового проекта, который может быть реализован при проведении лабораторных занятий по дисциплине «Прикладная химия» с целью подготовки студентов к реализации проектной деятельности в школе.

Одним из распространенных источников загрязнения природных водоемов выступают бытовые сточные воды, содержащие в своем составе большой набор органических веществ. Кроме того, органическое вещество может поступать в водоемы с поверхностным стоком с обрабатываемых сельскохозяйственных территорий, а также с водами животноводческих ферм. В итоге, природная вода, поступающая на дальнейшее использование, должна проходить предварительную очистку от органического вещества для дальнейшего использования в хозяйственных и производственных целях. В связи с этим, нами выбрана тема группового проекта «Способы очистки воды от органических загрязнителей».

Перед выполнением проекта перед обучающимися – студентами ставится проектная задача:

На одном из предприятий по очистке бытовых сточных вод произошла авария, которая привела к сбросу загрязненной воды в ближайший водоем. Водоем используется в системе питьевого водоснабжения. Необходимо определить, какой из методов будет

наиболее эффективным для очистки данной воды от сброшенного в нее органического вещества бытовых сточных вод?

После озвучивания задачи студентам предлагается самим сформулировать тему проекта, его цель и задачи, направленные на реализацию данной цели. Целью проекта является установление эффективного способа очистки воды от органических загрязнителей. Для достижения поставленной цели необходимо решить следующие задачи:

- познакомиться с методами, используемыми для очистки воды от органических соединений;
- провести очистку загрязненной воды используемыми способами и определить ее эффективность;
- сравнить результаты, полученные при очистке воды разными способами и сделать вывод о наиболее эффективном методе.

При выполнении работы аудитория делится на шесть групп. Каждая группа получает комплект материалов, включающий технологическую схему очистки водопроводной воды и выдержки из различных литературных источников, в которых описаны способы очистки воды от органических загрязнителей [2, 3,5]. После ознакомления с материалами и совместного обсуждения студенты приходят к выводу о распространенности применения для очистки от органических загрязнителей таких методов, как коагуляция и адсорбционная очистка.

В комплект раздаточного материала также входит методика определения показателя качества воды – химическое потребление кислорода (дихроматная окисляемость, или ХПК), выступающая в качестве одного из показателей, характеризующих количественное содержание органического вещества в воде [7]. После ознакомления с методикой проводится обсуждение, в рамках которого выделяются основные этапы выполнения работы:

1) определение количественного содержания органического вещества в загрязненной воде;
2) выполнение очистки воды от органического вещества с использованием предлагаемых методов;
3) определение содержания органического вещества после очистки;
4) сравнение полученных результатов и выделение метода, показавшего наибольшую степень очистки.

После этого каждой группе предлагается выбрать один из используемых на практике методов:

- очистка путем коагуляции с использованием сульфата алюминия;
- очистка путем коагуляции с использованием хлорида железа (III);
- очистка путем адсорбции на древесном угле;
- очистка путем адсорбции на активированном угле:
- очистка путем адсорбции на препарате «Полисорб».

Одна группа выполняет определение величины ХПК в загрязненной воде и проводит контрольный опыт по определению величины ХПК чистой воды. Кроме этого, данная группа получает для решения теоретические вопросы, ответы на которые раскрывают практическую значимость очистки воды от органического вещества.

1) В чем заключается негативная роль поступления органического вещества в водоемы?
2) В чем заключается опасность поступления органического вещества в водопроводную воду?
3) Объясните, почему в технологической схеме очистки водопроводной воды процесс коагуляции проводят раньше, чем операцию хлорирования?
4) Сточные воды бытового происхождения обогащены органическим веществом. Рассмотрите возможность их внесения на сельскохозяйственные поля для полива без предварительной очистки.

5) В какой период года природная вода нуждается в наибольшей степени очистки от органического вещества?

Для получения ответов на данные вопросы участникам также выдается методический материал из научных и научно-популярных источников информации [4,6,9].

Для выполнения исследования каждая мини-группа получает комплект лабораторной посуды (мерные, конические и круглодонные колбы, мерные пипетки, бюретку, стеклянные воронки, обратный холодильник), фильтровальную бумагу, электроплитки, реактивы для проведения очистки и анализа (сухие сульфат алюминия, хлорид железа (III), карбонат натрия, растворы серной кислоты, дихромата калия, соли Мора, фенилантраниловой кислоты), а также методику выполнения очистки. В качестве модельной системы бытовой сточной воды используется раствор органического вещества, например, гумата натрия, как распространенного загрязнителя природных вод.

По завершению анализа все результаты сводятся в единую таблицу, по результатам которой строится диаграмма, позволяющая сравнить эффективность очистки при реализации каждого из предполагаемых методов. В завершении проводится обсуждение полученных результатов, а также вопросов о роли органического вещества в природных водах и необходимости очистки от него. По итогам обсуждения делаются выводы о наиболее эффективных методах, реализуемых на практике для очистки вод от загрязнений органическим веществом.

Проект рассчитан на шесть академических часов в группе студентов 10-15 человек. Его выполнение позволяет студентам не только глубже познакомиться с методами очистки воды, но и освоить методику групповой проектной деятельности для ее дальнейшего использования в профессиональной деятельности педагога.

Список использованных источников

1) Газизова, Т.В. Подготовка студентов педагогического вуза к проектной деятельности / Т.В. Газизова, Т.А. Колесникова, А.И. Пеленков. // Сибирский педагогический журнал. – 2016. – № 1. – С. 79-85

2) Гетманцев, С.В. Система выбора эффективных технологий очистки природных вод с применением алюмосодержащих коагулянтов / С.В. Гетманцев // Водоснабжение и санитарная техника. – 2011. – №8. – С. 4-9.

3) Карпенко, А.В. Адсорбционные материалы для очистки сточных вод / А.В. Карпенко, Е.А. Татаринцева, В.А. Пемаев, Л.Н. Ольшанская // Техногенная и природная безопасность ТПБ-2013. Материалы II Всероссийской научно-практической конференции. – Саратов: КУБиК, 2013. – с. 76-80.

4) Карпенко, И.Л. Учебное пособие для студентов к практическим занятиям по разделу "Санитарная охрана почвы и очистка населенных мест" / И.Л. Карпенко, Л.А. Бархатова, Л.А. Перминова, Л.В. Зеленина. – Оренбург: Оренбургская гос. мед. академия, 2011. – 74 с.

5) Кульский, Л.А. Справочник по свойствам, методам анализа и очистке воды / Л.А. Кульский, И.Т. Гороновский, А.М. Когановский, М.А. Шевченко. – Киев: Наукова думка, 1980. – Т. 1. – 680 с.

6) Мельников, Е.А. Влияние городских бытовых сточных вод на окружающую среду, методы анализа и способы утилизации. / Е.А. Мельников // Дни науки студентов Владимирского государственного университета имени Александра Григорьевича и Николая Григорьевича Столетовых. Сборник материалов заочных научно-практических конференций. – Владимир, Владимирский гос. ун-т, 2020. – С. 1350-1358.

7) Муравьев, А.Г. Руководство по определению показателей качества воды полевыми методами / А.Г. Муравьев. – СПб.: «Крисмас+», 2004. – 248 с.

8) Тетюкова, А.П. Проектное обучение – инновационный подход к организации учебного процесса в высших учебных заведениях РФ / А.П. Тетюкова, Т.А. Белых // Физика. Технологии. Инновации. Сборник материалов VI Международной молодежной научной

конференции. – Екатеринбург: УрФУ им. первого Президента России Б.Н. Ельцина, 2019. – С. 349-358.

9) Филиппова, А.В. Влияние осадков бытовых сточных вод на видовое разнообразие почвенных организмов. / А.В. Филиппова, А.А. Мелько. // Вестник Оренбургского государственного университета – 2009. – № 6 (100). – С. 633-635.

ПАНДЕМИЯ COVID-19 В РАКУРСЕ ВИДЕНИЯ ЖИТЕЛЕЙ СТАРОГО ОСКОЛА

Воробьев Владислав Сергеевич, студент 2-го курса

Научный руководитель Канныкин Станислав Владимирович, доцент

Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования "Национальный исследовательский технологический университет "МИСиС", г. Старый Оскол

Актуальность работы обусловлена необходимостью осмысления реакции общества на государственные меры, связанные с преодолением пандемии COVID-19 и профилактикой заболевания короновирусом.

Объект исследования: общественное сознание жителей города Старого Оскола.

Предмет исследования: отношение жителей Старого Оскола к пандемии COVID-19 и государственным мерам по ее преодолению.

Цель исследования: выявление особенностей осмысления жителями Старого Оскола различных аспектов ситуации, связанной с пандемией.

Задачи исследования: 1. Анализ научной литературы и источников, выражающих общественное мнение по теме исследования (печатная и электронная пресса, интернет-ресурсы). 2. Составление опросника. 3. Проведение пилотажного исследования общественного мнения. 4. Интерпретация полученных результатов.

Методы исследования: теоретический анализ научной литературы, анкетирование, синтез и сравнение.

В проведенном опросе приняли участие 20 жителей Старого Оскола, из них мужчин – 4 (21%), женщин – 16 (79%). Имеют среднее образование – 1 (5%), среднее профессиональное – 2 (11%), среднее общее или получают высшее – 13 (68%), высшее – 3 (16%). Возраст опрашиваемых – от 17 до 28 лет.

Каждый вопрос сделан так, чтобы понять проблему граждан города. Для удобства было ответы были переделаны в обобщенный формат. Цели вопросов:

1. Как вы относитесь к вирусу? – вопрос дает понятие о том, как реагируют люди на данный вирус. Так по статистике было получено, что отрицательно – 12 (63%), нейтрально – 8 (37%).
2. Что предлагаете для борьбы с вирусом? – ответ на него дает возможность узнать если альтернативные методы борьбы у жителей города. Таким образом согласно статистике, было получено, что людей предлагающих носить маску и соблюдать правила поведения в период пандемии – 19 (95%), ничего не предлагаю – 1 (5%).
3. Как вы относитесь к масочному режиму? – результат ответа на него дает представление о том, как люди относятся к режиму, которого раньше не было. Таким образом по статистике мы можем наблюдать, что ответили положительно – 7 (37%), в целом положительно – 3 (16%), нормально – 3 (16%), нейтрально – 2 (10%), отрицательно – 4 (21%).
4. Легко ли вам было привыкнуть к изменениям? – ответ на него дал возможность делать выводы на состояние опрашиваемого в начале пандемии. Так по статистике было получено, что ответили да – 11 (58%), нет – 9 (42%).
5. Каким источникам новостей о коронавирусе вы доверяете? – вопрос дает понять каким источникам информации люди доверяют и делать вывод о загрязненности ее различными фейками. Таким образом согласно статистике, было получено, что официальные сайты, региональные оперштабы – 10 (50%), интернет – 8 (40%), телевидение – 2 (10%).
6. По какому принципу вы отбирает информацию из информационных источников? – исходя из полочных ответов на него дает понять способность людей отбирать среди фейковой и истинной информации. Таким образом по статистике мы можем

наблюдать, что критически подхожу при выборе информации. Из большого потока беру только ту которая обоснована и не имеет после ее прочтения никаких остаточных вопросов – 11 (55%), сравниваю информацию, которая поступает мне из телевидения и социальных групп с разговорами от людей – 5 (25%), особо не задумываюсь беру то, что предлагает моя подписка на различные социальные группы и телевидение – 4 (20%).

7. Какие еще знаете слухи, заговоры, мифы, которые могли слышать от других людей в нашем городе? - ответ на него дал возможность делать выводы присутствуют ли в городе фейковая информация. Таким образом согласно статистике, было получено, что да – 7 (37%), нет – 13 (63%).

Результаты исследования позволили прийти к следующим выводам: 1. В основном респонденты рассматривают пандемию как проявление халатности ученых, изучающих вирусы и допустивших их утечку из лаборатории. **2.** В лечении и профилактике заболеваемости респонденты доверяют в первую очередь рекомендациям знакомых, особенно тех, кто переболел COVID-19, и отмечают недостаточную готовность медицинских работников и учреждений к деятельности в ситуации пандемии. **3.** Масочно-перчаточный режим первое время доставлял неудобства респондентам, некоторые из них до сих пор имеют сомнения в его эффективности. Однако большинство опрошенных уже привыкли к нему и относятся в целом нейтрально. **4.** Первоначальное осмысление ситуации пандемии и привыкание к ограничительным мерам было сопряжено у многих респондентов с эмоциональным угнетением, связанным с опасениями за свою жизнь и здоровье, благополучие родных и близких людей, а также в связи с угрозой потери работы или резкого ухудшения материального положения. **5.** Множество мифов, которые возникли в самом начале пандемии, уже не вызывают интереса. Большинство респондентов склонны доверять профессиональным СМИ, осуществляющим фактчекинг. **6.** Характеристики респондентов, участвовавших в пилотажном исследовании и связанные с их возрастом, полом и образованием, на момент проведения исследования не играли существенной роли в различии восприятия ситуации с пандемией. **7.** Мы полагаем, что лучшим способом борьбы с паникой, стрессом и мифами в ситуации пандемии является доступное для понимания «обычного» человека, своевременное и достоверное информирование населения.

Список использованных источников

1. Чистякова Н.В., Айсувакова Т.П. — Метакогнитивная модель совладающего поведения субъекта в период эпидемии Covid-19 // Психолог. – 2020. – № 3. DOI: 10.25136/2409-8701.2020.3.33033 URL: https://nbpublish.com/library_read_article.php?id=33033

2. Калякина Инесса Македоновна, Аванесян Эрик Артурович, Сайфуллин Айнур Саматович Влияние Covid-19 на экономику России // Московский экономический журнал. 2020. №6. URL: https://cyberleninka.ru/article/n/vliyanie-covid-19-na-ekonomiku-rossii (дата обращения: 11.01.2021).

3. О. А. Левшукова, А. С. Матвеев, Д. П. Позоян Возможные последствия пандемии COVID-19 на развитие экономики России // ЕГИ. 2020. №3 (29). URL: https://cyberleninka.ru/article/n/vozmozhnye-posledstviya-pandemii-covid-19-na-razvitie-ekonomiki-rossii (дата обращения: 11.01.2021).

4. Ефремова Диляра Набиулловна Дыхание коронавируса: об осуществлении дистанционной психологической помощи в период пандемии // Вестник МГОУ. 2020. №2. URL: https://cyberleninka.ru/article/n/dyhanie-koronavirusa-ob-osuschestvlenii-distantsionnoy-psihologicheskoy-pomoschi-v-period-pandemii (дата обращения: 11.01.2021).

5. Федоров Александр Викторович, Левицкая Анастасия Александровна, Новиков Андрей Сергеевич Коронавирус как источник медийных манипуляций // Crede Experto: транспорт, общество, образование, язык. 2020. №2. URL: https://cyberleninka.ru/article/n/koronavirus-kak-istochnik-mediynyh-manipulyatsiy (дата обращения: 11.01.2021).

6. Очергоряева Джиргал Викторовна Ксенофобия как конфликтогенный фактор социальной напряженности в условиях пандемии коронавируса // Обзор НЦПТИ. 2020. №3 (22). URL: https://cyberleninka.ru/article/n/ksenofobiya-kak-konfliktogennyy-faktor-sotsialnoy-napryazhennosti-v-usloviyah-pandemii-koronavirusa (дата обращения: 11.01.2021).

7. Лубеницкая А.Н., Иванова Татьяна Ильинична Мир уже никогда не станет прежним - пандемия нового тысячелетия (обзор литературы) // Омский психиатрический журнал. 2020. №S2-1 (24). URL: https://cyberleninka.ru/article/n/mir-uzhe-nikogda-ne-stanet-prezhnim-pandemiya-novogo-tysyacheletiya-obzor-literatury (дата обращения: 11.01.2021).

8. Садыков Д.И. Пандемия COVID-19 как вызов современной демократии // Скиф. 2020. №4 (44). URL: https://cyberleninka.ru/article/n/pandemiya-covid-19-kak-vyzov-sovremennoy-demokratii (дата обращения: 11.01.2021).

9. Дейнека О. С., Духанина Л. Н., Максименко А. А. Фейки и особенности их распространения в СМИ и социальных сетях в период инфодемии, вызванной covid-19 //European Scientific Conference. – 2020. – С. 326-340 (дата обращения: 11.01.2021).

10. Семенова Е. А. Новые городские медиа и их влияние на общественные и семейные ценности (на примере работы тамбовских СМИ в период пандемии COVID-19) (дата обращения: 11.01.2021).

УПРАВЛЕНИЕ ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ СТУДЕНТОВ В СТРУКТУРЕ МЕНЕДЖМЕНТА КОЛЛЕДЖА

Григорьева Любовь Владимировна, аспирант 2-го курса
Шаповалов Валерий Кириллович доктор педагогических наук, профессор, заведующий кафедрой «Теория и методика профессионального образования
Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет», г. Ставрополь, Россия

Изменения последних лет в области российского профессионального образования ставят перед руководителями образовательных учреждений новые управленческие задачи. Одна из задач образовательного учреждения состоит в том, чтобы сократить период адаптации студентов к учебно-исследовательской и научной работе. Решение этой задачи возможно в том случае, если с первых дней пребывания в колледже студент будет активно участвовать в разнообразных формах научной работы, проводимых кафедрами (отделениями, методическими объединениями). Успешность и результативность такой адаптации наряду с другими факторами обусловлена созданием органов управления, которые призваны определить цель, задачи, основные направления научной деятельности, формы, методы и средства их реализации. Внутриколледжное управление системой учебно-исследовательской деятельности студентов должно скоординировать деятельность преподавателей и мастеров, работающих со студентами на одном курсе, руководителей производственных практик и представителей вуза, выступающих в качестве научных экспертов учебных исследований.

Внутриколледжное управление системой учебно-исследовательской деятельности студентов следует понимать как непрерывную последовательность действий, осуществляемых должностными лицами, органами управления, структурными подразделениями колледжа. Они призваны разработать и обеспечить стабильное функционирование и устойчивое развитие целостной совокупности содержания, методов и форм организации совместной деятельности преподавателей и студентов по овладению системой знаний, умений, процедур творческой деятельности, ценностных ориентаций, позволяющих корректно осуществлять учебное исследование.Специфика учебно-исследовательской деятельности студентов предполагает, что управление будет основано на следующих принципах: системном, деятельностном, квалиметрическом, синергетическом и принципе субъект-субъектных отношений.

Необходимым фактором функционирования системы управления учебно-исследовательской деятельностью студентов является видение связей между частями системы. Понятие «система» означает цельный, единый инструмент, в котором возможно выделить отдельные части. В управлении исследовательской деятельностью как системой важно видеть не только основные части системы, но и те связи и отношения, которые возникают, складываются или разрушаются между этими частями. Другими словами, какие компоненты системы выступают в качестве системообразующих, такова и перспектива развития связей и отношений системы. Наличие структуры составляет признак системы. Система интергративна, это объясняется тем, что каждый элемент обладает своими качествами и присущими ему свойствами, при их взаимодействии образуются новые связи, компоненты, которые не сводятся к прежним.

Устойчивость интегративного свойства определяется целостностью системы. В управлении важно помнить и о ее тесной и специфической связи с внешней средой, которая оказывает сильное воздействие.

Важно, чтобы процесс управления учебно-исследовательской деятельностью студентов был оптимальным и целостным, т.е. после выявления всех связей выбирались те из них, которые позволяют добиться поставленных целей. Целостность будет выступать внутренним единством системы управления учебно-исследовательской деятельностью учащихся.

Деятельностный подход к управлению подразумевает, что процессы обучения и воспитания не сами по себе непосредственно развивают человека, а лишь тогда, когда они имеют активные формы и обладают соответствующим содержанием, в нашем случае в старшем школьном возрасте формируются те или иные умения, согласно ведущим типам деятельности. Следовательно, ориентируясь на ведущий тип деятельности старшеклассника, организация материала, предоставляющая ученику возможность выбора содержания, методов поиска и переработки учебных знаний, стимулирует развитие исследовательской направленности в деятельности учащихся.

Как уже отмечалось выше, для успешного ведения в колледжах и техникумах научно-исследовательской работы студентов преподаватель СПО должен представлять структуру научно-исследовательской деятельности студентов в условиях СПО, а также знать общие принципы ведения научной работы применительно к условиям своего труда.

В основу определения содержания функций внутриколледжного управления системой учебно-исследовательской деятельности студентов в условиях профессионального обучения нами положена точка зрения Ю.А. Конаржевского [1] и Т.И. Шамовой [2] на управленческий цикл, который представляет собой: анализ, планирование, организация, контроль, регулирование.

Структура управления согласно функциям, где управление разделено на функциональные службы, за каждой из которых закреплен определенный круг работ, в большей мере соответствует такому объекту как развитие исследовательской компетентности студентов, так как предполагает вовлечение в этот процесс значительного количества преподавателей и мастеров, создания и освоения нововведений, требующих компетентных решений, учитывающих мнение большинства членов педагогического коллектива. Это предполагает взаимную согласованность деятельности традиционных методических объединений преподавателей, структурных подразделений колледжа, обеспечивающих стабильность образовательного процесса, и временных групп преподавателей, инновационных органов управления, способствующих развитию образования, что обеспечивает достижение, с одной стороны, оперативности и простоты, а с другой – коллегиальности и компетентности внутриколледжного управления системой учебно-исследовательской деятельности студентов.

При организации и проведении научно-исследовательской деятельности определяются основополагающие принципы исследования:

- единство и активное взаимодействие научно-исследовательской, инновационнно-проектной и образовательной деятельности;
- направленность на социальное и духовное развитие личности;
- концентрация усилий и ресурсов на приоритетных, социально значимых и недостаточно освоенных направлениях;
- поддержка и развитие научного творчества обучающихся;
- поддержка ярких творческих индивидуальностей, способных обеспечить высокий уровень проводимых исследований;
- доведение результатов исследований и проектов до применения в практической деятельности, используя при этом издательскую деятельность и возможности сети Интернет;
- развитие многообразия форм организации научно-исследовательской и творческой деятельности.

Проблемы, с которыми приходится сталкиваться при организации НИРС:

1. Слабая ресурсная база (материально-техническая): уменьшение денежных средств на подписку, покупку литературы, лабораторного оборудования.

2. Отсутствие связи с работодателями, что затрудняет получение информации.

3. Недостаточная мотивация студентов и преподавателей.

4. Неотработанность новой системы оплаты труда педагогических работников в соответствии с задачами инновационного развития.

5. Слабая подготовленность студентов к научно-исследовательской работе.

Пути решения данных проблем следующие:

- ввести в учебный план спецкурс «Основы научно-исследовательской деятельности студентов»;
- научно-исследовательская деятельность должна быть непрерывная, начиная с 1 курса и до окончания обучения;
- заниматься ею должны все преподаватели, и при этом необходимо учитывать её результаты при аттестации педагогических работников;
- за системность в работе требуется материально поощрять преподавателей;
- подбирать индивидуальные формы научно-исследовательской деятельности для каждого студента;
- осуществлять поиск спонсоров и социальных партнёров.

Масштабность и эффективность проектно-исследовательской деятельности студентов под руководством преподавателей во многом определяется ее моральным стимулированием и материальным вознаграждением.

Исследовательская компетенция считается метапредметной и включает в себя комплекс образовательных компетенций, напрямую связанных с мыслительными, поисковыми, логическими, творческими процессами познания студентов. В рамках освоения учебных дисциплин и профессиональных модулей формирование этой компетенции не может быть эффективно осуществлено. Необходимо введение внеаудиторной занятости в виде изучения курса или дисциплины.

Исследовательская деятельность имеет свои формы и методы. Она может носит аудиторный и внеаудиторный характер. Выполнение НИР представляет собой совокупность различных форм: работа в студенческих кружках, участие в исследованиях, проводимых студентами техникума; исследовательская работа, проводимая по индивидуальному плану; участие в научно-теоретических конференциях, выступления с докладами и сообщениями по материалам собственных исследований.

При формировании исследовательских навыков введения научно-исследовательской работы нужно понимать, что научно-исследовательской деятельностью должен заниматься каждый студент, это не должно носит характер выделения сильных обучающихся.

Внутриколледжное управление системой учебно-исследовательской деятельности студентов должно скоординировать деятельность преподавателей и мастеров, работающих со студентами на одном курсе, руководителей производственных практик и представителей вуза, выступающих в качестве научных экспертов учебных исследований.

Список использованных источников

1. Конаржевский Ю.А. Менеджмент и внутришкольное управление. – М.: Центр «Педагогический поиск», 1999. – 224 с.Шамова Т.И. Исследовательский подход в управлении школой. – М.: АПП ЦИТП, 1992. – 66 с

2. Шепелев М.В., Румянцев Е.В., Вашурин А.С. Организация научно-исследовательской деятельности учащихся в системе «Школа – вуз»: Опыт регионального университета. Известия высших учебных заведений. Гуманитарные науки, 2013, т. 4.№ 3, с. 210–214.

3. Широбокова Т.С. Организация и проведение исследовательской деятельности обучающихся в образовательных учреждениях системы СПО / Т.С. Широбокова // Научные исследования в образовании. – 2011. – № 7.

4. Шихова, А.Л. Организация исследовательской деятельности студентов колледжа / А.Л. Шихова //Сборник материалов по итогам областного студенческого форума: сб.ст./ под общ.ред. М.Ю. Козловой. – Киров: Изд-во ООО «Радуга-ПРЕСС», 2012.-114

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ДИАГНОСТИРОВАНИЯ НЕИСПРАВНОСТЕЙ КОМПЬЮТЕРНОЙ ТЕХНИКИ И КОММУНИКАЦИОННОГО ОБОРУДОВАНИЯ

Давыдова Кристина Алексеевна, студентка второго курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС» Оскольский политехнический колледж, г. Старый Оскол

Аннотация: В данной статье рассматривается проблема установления причины неисправности компьютерной техники и коммуникационного оборудования на предприятии с использованием ЭВМ.

Ключевые слова: экспертная система, форма, проблема, система управление базой знаний, приложение, специалист.

Актуальностью данной работы заключается в том, что на данный момент на предприятии отсутствует специализированное программное обеспечение, которое позволило бы определить причину неисправностей компьютерной техники и коммуникационного оборудования без вызова специалиста.

В настоящее время на предприятии ремонт компьютерной техники и коммуникационного оборудования осуществляется только через специалиста, что является достаточно времязатранным процессом. Наличие экспертной системы на предприятии позволит сократить время устранения неисправностей в работе компьютерной техники и коммуникационного оборудования.

Целью работы является разработка экспертной системы диагностирования неисправностей компьютерной техники и коммуникационного оборудования.

Для автоматизации диагностирования неисправностей в работе компьютерной техники и коммуникационного оборудования необходимо разработать экспертную систему. Разрабатываемая система должна:

- заносить информацию в созданную базу;
- выполнять необходимые действия по модификации и удалению информации в базе;
- поддерживать целостность базы данных, не допуская появления некорректных данных;
- содержать достаточное количество данных, позволяющее продемонстрировать результаты работы с экспертной системой;
- предоставлять справочную информацию по запросу пользователя;
- обеспечивать разграничение прав доступа.

Функционирование любого программного обеспечения невозможно без информационных потоков, которые можно разделить на две большие группы:

входная информация – это информация, которую получает человек или устройство. В качестве входной информации для данной предметной области, выступают:

- данные об оборудовании;
- данные о неполадках в работе компьютерной техники и коммуникационного оборудования;
- возможные варианты решения проблемы;
- результат решенной проблемы.

Выходная информация – это информация, которая получается после обработки человеком или устройством входной информации [1].

В качестве выходной информации для данной предметной области, выступает:

- результат решенной проблемы;

- отчет о решенных проблемах с указанием выбранного варианта устранения возникшей неисправности.

В качестве документов, регламентирующих процессы предметной области, выступает:

- инструкция пользователя.

В качестве механизмов, осуществляющих данные бизнес-процессы предметной области, выступают:

- пользователи;
- экспертная система.

Для создания информационной системы была выбрана Microsoft SQL Server 2012. Данная СУБД отличается своей надежностью, мощностью в производительности.

Во время разработки приложения были созданы формы. На рисунке 1 показана главная форма приложения для перехода ко всем последующим формам. Данная форма представлена в режиме конструктора.

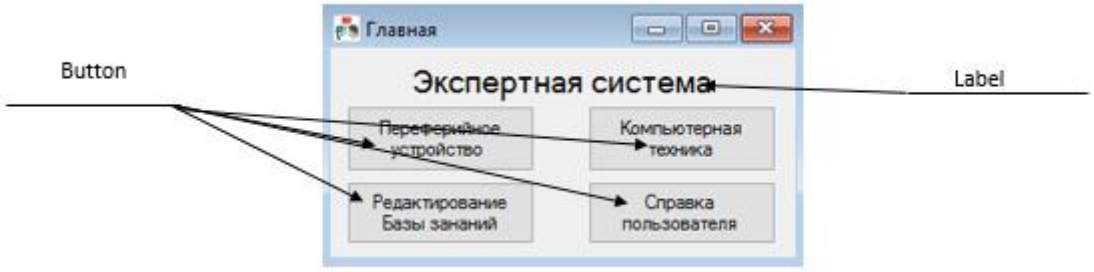


Рисунок 1 – Главная форма

На рисунке 2 представлена форма по выявлению проблемы периферийного устройства. Форма в режиме конструктора.

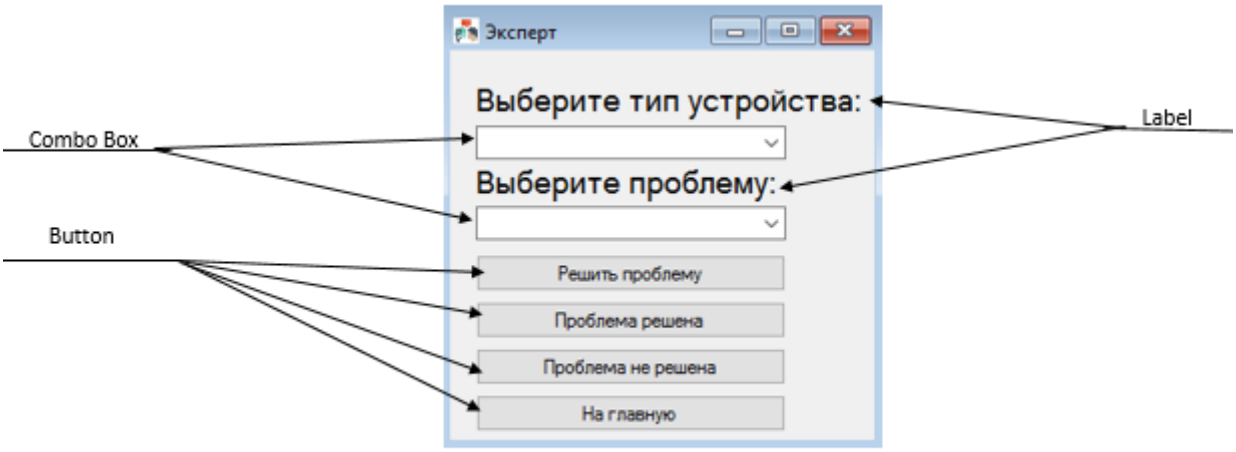


Рисунок 2 – Форма по выявлению проблемы периферийного устройства

Информационная безопасность является неотъемлемой частью каждого предприятия, так как она отвечает за сохранность данных и конфиденциальной информации предприятия, то есть информационная безопасность – это процесс обеспечения конфиденциальности, целостности и доступности информации [4].

Обмен информацией в организации осуществляется посредством локальной вычислительной сети.

Схема ЛВС с наличием предположительных угроз показана на рисунке 3.

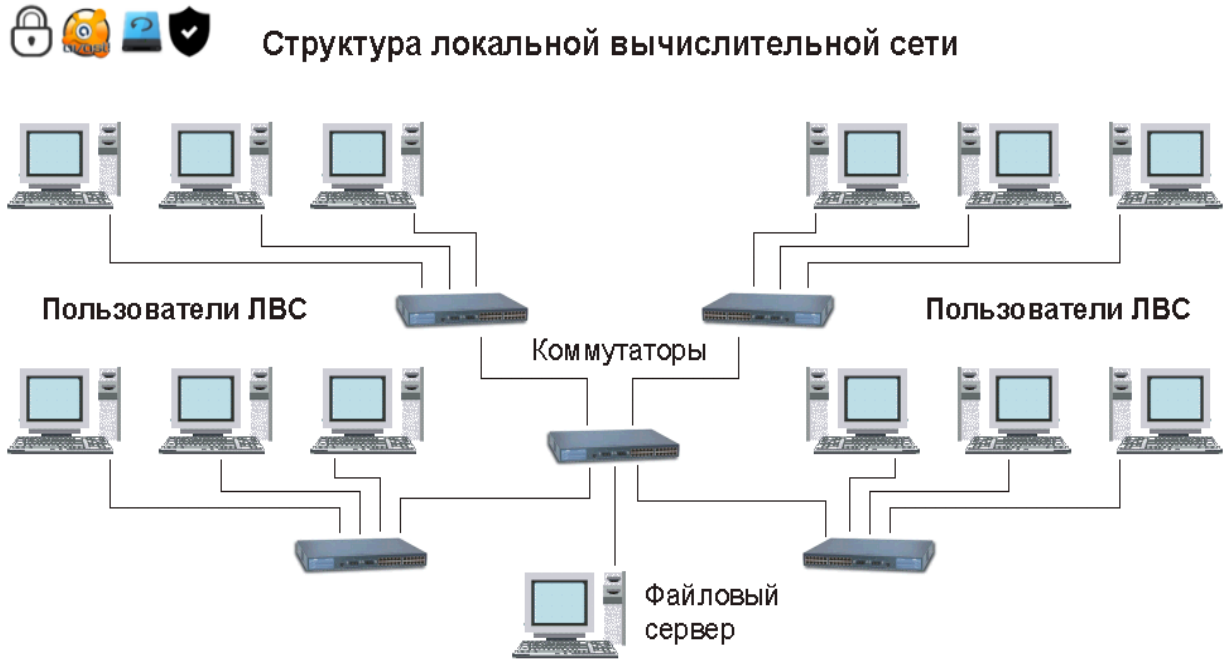


Рисунок 3 – Схема ЛВС с наличием предположительных угроз

Информационная безопасность обеспечивается следующим образом:

- защита паролем клиента и сервера;
- резервное копирование данных на сервере;
- разграничение доступа к данным в клиентском приложении;
- обеспечение аутентификации системы;
- использование средств антивирусной защиты;
- использование брандмауэра.

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. – М.: ФОРУМ: ИНФРА-М, 2017. – 368с.

2. ГроффДж.Р., Вайнберг П.Н., ОппельЭ.Дж. SQL. Полное руководство. – М.: Вильямс, 2015. – 959 с.

3. ШарпДж. MicrosoftVisualC#: Питер, 2017. – 848 с.

4. Баранова, Е. К. Информационная безопасность и защита информации: Учебное пособие / Баранова Е. К., Бабаш А. В. – 3-е изд. - Москва : ИЦ РИОР, НИЦ ИНФРА-М, 2016. - 322 с.

5. Портал электронного обучения ОПК СТИ НИТУ «МИСиС»: [Электронный ресурс]. – http://www.unami.ru/

6. Сайт для программистов C#: [Электронный ресурс]. – http://www.programmer-lib.ru/csharp.php

7. Сайт АО «КМА руда»: [Электронный ресурс]. – http://kmaruda.ru/

8. Сайт антивируса Касперского: [Электронный ресурс]. - https://my.kaspersky.com/?returnUrl=http%3a%2f%2fmy.kaspersky.com%2fMyLicenses

9. Сайт Представления знаний в интеллектуальных системах, экспертные системы: [Электронный ресурс]. – https://habr.com/ru/post/346236/

ДЕАЭРАТОР

Мищенко Светлана Михайловна, студентка 4-го курса
Научный руководитель Канайчева Ольга Васильевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Одной из актуальнейших проблем теплоэнергетики является защита оборудования, трубопроводов тепловых электрических станций и сетей теплоснабжения от коррозии.

Для котельных, обслуживающих теплосети, деаэрация воды является подготовительным процессом. Это мероприятие позволяет обезопасить теплоноситель, исключая из его состава вредоносные компоненты, которые снижают срок службы оборудования.

Деаэрация – процесс удаления кислорода и других газов с водных сред. Коррозия в деаэрированной воде сводится к минимуму, поэтому деаэрация является эффективным практическим средством защиты металла от коррозии в пресной и морской воде.

Вакуумный деаэратор, как и атмосферный, состоит из колонки и бака деаэрованной воды, только с той разницей, что бак и колонка находятся в различных местах: бак – на нулевой отметке, а колонка – выше крыши котельной.

На первой стадии процесса деаэрации вода подается в подогреватель, а затем проходит через фильтры, осуществляющие химическую очистку. Следующей на пути воды находится деаэрационная колонна, специально предусмотренную в деаэраторе для высвобождения газов. На последнем этапе подпиточный насос переправляет очищенную воду в накопительный резервуар, откуда она подается в систему. Все же этого недостаточно для полного высвобождения активных составляющих теплоносителя. Поэтому на следующем этапе очистки применяют различные реагенты, способные связывать кислород. Для разогретого теплоносителя хорошо подходит сульфит натрия, реакция которого усиливается в данных условиях. В некоторых случаях для ускорения реакции используют различные катализаторы. Контакт воды с металлической стружкой обеспечивает высвобождение излишних молекул кислорода, в результате окисления стружка превращается в ржавчину.

Областью для проектирования, монтажа и эксплуатирования вакуумного деаэратора являются водогрейные котельные (особенно в блочном варианте) и тепловые пункты. Так же вакуумные деаэраторы активно используются в пищевой промышленности для деаэрации воды необходимой в технологии приготовления широкого спектра напитков.

Для эффективной работы котла важно неукоснительно соблюдать правила безопасной эксплуатации, которых требует деаэрационная установка. Показания приборов необходимо регистрировать несколько раз в течение смены, для возможности расчета состояния деаэратора. Для химических реагентов следует составлять указанные пропорции, регулярно брать на пробу очищенную воду и контролировать ее уровень в баке. Чтобы сбои не происходили из-за ошибок в показаниях измерительных приборов или автоматики, оборудование подвергается систематическому осмотру, периодичность которого регламентируется в технической документации.

Список использованных источников

1. Иваненко А.С. Водоподготовка. Пособие аппаратчику. Киев: Тэхника, 1978. - 184 с.
2. Шарапов, В.И. Термические деаэраторы / В.И. Шарапов, Д.В. Цюра. - Ульян. гос. техн. ун-т., 2003. - 560 с.
3. Оликер, И.И. Термическая деаэрация воды в отопительно-производственных котельных и тепловых сетях [Текст] / И.И. Оликер. - Л.: Стройиздат, 1972. - 137 с.

4. Теплоэнергетика и теплотехника [Текст]: в 3 кн. Кн. 1. Теплоэнергетика и теплотехника: Общие вопросы: Справочник / Под общ. ред. чл.-корр. РАН А.В. Клименко и проф. В.М. Зорина. - 3-е изд., перераб. - М.: Изд-во МЭИ, 1999. – 528 с.

ЭЛЕВАТОРНЫЙ УЗЕЛ

Одиноков Иван Александрович, студент 4-го курса
Научный руководитель Канайчева Ольга Васильевна,
преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Элеваторный узел – это специализированное оборудование, располагающееся в тепловом распредпункте. Основные задачи этого устройства: увеличение объёма нагреваемой воды, уменьшение её давления и t, а также перекачка. Регулировка работы обычных элеваторов происходит путём уменьшения или увеличения размеров составных частей. Также существуют механически и электрически регулируемые элеваторы.

Элеваторный узел системы отопления – особый функциональный механизм, который является частью отопительного оборудования дома. По сути он выполняет роль водоструйного или эжекционного насоса.

Благодаря своему устройству элеватор позволяет повышать давление в теплосистеме, повышая при этом объём теплоносителя (повышение количества воды получается из-за её большой температуры и такого же большого давления). Это значит, что вода в трубах нагревается до 150°С, не превращаясь при этом в пар из-за закрытого пространства. Кроме этого, в элеваторе генерируется повышенное давление. Все указанные условия, которые создаёт элеваторное устройство, способствуют последующей более эффективной подаче тепла в отопительные трубы.

После того, как 150-градусная вода подошла к месту её непосредственного использования включается элеватор. Он должен понизить температуру и давление воды, ведь в таком разогретом состоянии теплоноситель не может поступать в отопительные системы. В противном случае чугунные батареи, трубы при этом испортятся и при этом даже сохранится вероятность их разрыва, что может иметь печальные последствия. Даже если радиаторы не чугунные, а сделаны из другого металла, есть вероятность получить ожог.

Принцип работы элеватора таков: в: сначала нагретая вода из общей магистрали поступает в патрубок рассматриваемого устройства.

Так как теплоноситель находится под давлением, он перемещается чуть дальше, проходя сквозь узкое сопло. При этом возникает эффект инжекции или эффект Вентури, то есть в следующей камере (приёмной) создаётся зона разряжения. Так как указанная камера имеет пониженное давление, начинает действовать закон термодинамики и холодная вода из другого патрубка начинает засасываться в эту часть элеваторного узла. Второй патрубок подключён к так называемой трубе обратки.

В результате вышеописанных процессов в следующей части приспособления, которая называется смесительной горловиной, горячая и холодная вода перемешиваются, а давление снижается. После этого нормальной температуры жидкость отправляется непосредственно в систему, обогревающую дома в зимний период.

Таким образом, кроме снижения рабочих параметров системы, элеватор выполняет также функцию насоса. Одна из важнейших задач, которые решает элеватор, – создание необходимого и подходящего давления, которое может преодолеть водяное сопротивление тёплой системы дома. Для этого вертикальная перемычка на месте стыка врезается под углом 45^0. Это способствует лучшему разделению водяных потоков.

Устройство элеватора содержит другие важные и важные для теплоснабжения элементы. Это приспособление также оснащается фильтрами и обвязкой, в которую входят:

- манометры (для контроля системного давления);
- фильтры (освобождают от грязи);
- термометры (для контроля температуры; располагаются сразу в трёх местах системы);

- задвижки (нужны для доступа внутрь системы, а также для осуществления аварийных и других работ).

Фильтры, используемые в элеваторе, могут быть двух типов: грязеуловительные или сетчато-магнитные. Первые удаляют наиболее крупный мусор из теплоносителя, вторые отвечают за очистку воды, которая поступает в домовые радиаторы отопления и трубы.

Рассмотрим, для чего нужен элеватор. Это приспособление находит применение в основном в централизованных системах отопления, а именно там, где t поднимается до ста пятидесяти градусов Цельсия, давление составляет 6-10 бар. Это необходимо для того, чтобы:

- оборудование, работающие с высокими температурами, функционировало исправно и с высоким коэффициентом полезного действия;
- доставлять достаточно нагретую воду в отдалённые от котельной районы;
- экономить ресурсы (за счёт того, что вода, нагретая до температуры более 100°С и имеющая повышенное давление, содержит больше тепловой энергии, чем более холодная, например, девяностоградусная).

Практика использования элеваторов отопления показывает, что применение регулируемых устройств больше нужно для зарубежных реалий: российские холодные зимы обычно требуют хорошего, стабильного обогрева жилых помещений и постоянно изменять температуру теплоносителя не требуется.

Также регулирующиеся элеваторы находят своё применение для обогрева нежилых помещений: если снизить температуру на ночь, когда клиентов и посетителей нет, можно добиться экономии до 30%. Регуляция теплоносителя с помощью такого элеватора отопления осуществляется с помощью специального дополнительного реле, оснащённого электроприводом.

Список использованных источников

1. Абрамов А.И., Елизаров Д.П., Ремезов А.Н., Седлов А.С. и др. Повышение экологической безопасности тепловых электростанций: учеб, пособие / под ред. А.С. Седлова. М: Изд-во МЭИ, 2001. 378 с.
2. Белосельский Б.С., Александров А.А., Клименко А.В. и др. Теплоэнергетика и теплотехника: справочник. М.: Издательский дом МЭИ, 2007. 564 с.
3. Данилов О.Л., Гаряев А.Б., Яковлев И.В. и др. Энергосбережение в теплоэнергетике и теплотехнологиях: учебник для вузов / под ред. А.В. Клименко. 2-е изд., стер. М.: Издательский дом МЭИ, 2011. 424 с.

СПОСОБЫ И МЕТОДЫ ПРОТИВОАВАРИЙНОЙ ЗАЩИТЫ КОТЕЛЬНЫХ

Полянский Евгений Максимович, студент 3-го курса
Научный руководитель Сальков Вадим Анатольевич, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Перед работой котельных установок одними из важных мероприятий охраны труда являются тренировки по противопожарной и противоаварийной безопасности.

Ведется журнал учета проведения противоаварийных и противопожарных тренировок, позволяющих фиксировать и упорядочить эти процедуры.

Поведение противоаварийных тренировок регламентировано нормативными документами, в том числе правилами промбезопасности.

Перед выполнением обязательно должны быть подготовлен - график проведения тренировочных занятий. В этом документе указываются темы, даты и время проведения. На основании утвержденного графика заполняется журнал проведения занятий.

Любой котлоагретат допускается к работе только после освидетельствования и получения разрешения на ввод в эксплуатацию. Перед растопкой котла тщательно осматривают оборудование на исправность и работоспособность. Рабочий персонал должен ежечасно следить за оборудованием котельной, работой приборов КИПиА, подачей топлива и т.д.

Котельные должны быть обеспечены рабочим и аварийным электрическим освещением. Аварийное освещение должно обеспечивать беспрепятственное наблюдение за показаниями контрольно-измерительных приборов, состоянием оборудования и коммуникаций, а также возможность необходимых переключений при аварийных ситуациях.

Также немаловажным фактором является микроклимат котельной (влажность, температура, давление и др.).

В заключении я хочу сказать, что современные котельные оснащены автоматизированными технологиями, которые позволяют качественно, безопасно и быстро произвести автоматическое отключение подачи топлива и воды. Реконструкция котельных - это полная или частичная замена изношенного котельного оборудования на новое, техническое совершенствование теплового источника, оптимизация работы системы в целях повышения эффективности работы установки, снижения эксплуатационных затрат и приведения котельной в полное соответствие современным требованиям.

Использование устаревшего оборудования приводит к перерасходу топлива и высокой себестоимости отпускаемой тепловой энергии, так как оборудование изношено, не отвечают современным требованиям, и поэтому работает с низким КПД. Замена устаревших котлов на новые под силу не всем, однако можно внедрить новое оборудование, что позволит снизить расход топлива, сократить выбросы вредных веществ в атмосферу и повышению КПД котла. Устаревшее оснащение не отвечает современным требованиям, становится причиной частых поломок, приводит к увеличению расходов на ремонт и содержание котельных.

Работы по модернизации котельных позволят не только увеличить производительность, но избежать выхода оборудования из строя и аварийных ситуаций, которые могут за этим последовать.

Список использованных источников

13. Инструкция по охране труда для слесаря-ремонтника. - ИОТ ВЧДР-17-076-2016 03.11.2016.

14. Инструкция по охране труда для мастера (старшего мастера). - ИОТ-ВЧДР-17-003-2016 24.06.2016.

15. Инструкция по охране труда для работников, выполняющих уборку рабочих мест территорию депо. - ИОТ-ВЧДР-17-008-2016 21.11.2016.

16. Инструкция по охране труда для оператора котельной. - ИОТ-ВЧДР-17-083-2019 21.06.2019.

17. Инструкция по охране труда для аппаратчика химводоочистки. - ИОТ-ВЧДР-17-082-2019 21.06.2019.

18. Инструкция по использованию средств индивидуальной защиты. - ИОТ-ВЧДР-17-004-2019 30.01.2019.

19. Инструкция по оказанию первой помощи пострадавшим. - ИОТ-ВЧДР-17-011-2019 03.12.2019.

20. Инструкция по охране труда при нахождении на железнодорожных путях. - ИОТ-ВЧДР-17-046-2019 30.01.2019.

ПРОБЛЕМА ВОДОПОДГОТОВКИ И ВОДООЧИСТКИ ПРИ РАБОТЕ КОТЕЛЬНОЙ

Пономарева Мария Александровна, студентка 3-го курса
Научный руководитель Сальков Вадим Анатольевич, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

С самого начала я рассмотрела, какие процессы производятся с водой при поступлении в котельную.

В котельной в зависимости от типа воды используются различные очистные установки.

Химическая водоочистка (ХВО) – это совокупность мер докотловой котельной с целью удаления из воды накипи образующих солей жесткости.

При питании котлов жесткой водой на стенках барабанов, коллекторов и труб откладывается накипь, составные соединения которой крепко соединяются с поверхностью металла. Накипь и шлам имеют низкую теплопроводность, в результате чего ухудшается теплопередача через загрязненные стенки.

Химводоочистка (ХВО) для котельных предназначена для снижения жесткости воды и ее умягчения, а также очищения воды от вредных примесей. В основном в ХВО используют солевые растворы с добавлением других примесей. Со временем ХВО изнашивается, и для полного восстановления применяются специальные регенеративные комплексы. Например, регенерация исходной водой с добавлением 26% раствора соли.

Комплексы ХВО является важным режимом работы для снабжения котельной умягченной водой.

Поскольку сточные воды котельной содержат в себе много различных примесей, например, таких как реагенты и соли, в следствие они приводят к существенному повышению солесодержания водоемов и изменению показателя ПДК. Для исключения вредного влияния на окружающую среду (в частности, водоемы) количество содержащихся в сточных водах примесей не должно превышать установленные санитарными нормами ПДК.

Вследствие изучения сточных вод выяснено, что проблема водоочистки заключается в том, что вода недостаточно хорошо очищается при сбросе в сточные воды.

Комплекс очистки сточных вод проводится перед спуском жидкости в водоемы. Если мероприятиями пренебречь, загрязнения попадут в природный водоем и почву, и отравят локальную экосистему. Численность растений и животных уменьшится. Опасные вещества накапливаются в экосистеме и по пищевой цепи попадают в организм человека.

В ходе изучения проблемы водоподготовки и водоочистки при работе котельной для предотвращения образования накипи, коррозионных процессов и продления срока службы используют химическую водоподготовку воды. Аппаратчик химводоочистки напрямую связан с экологическим состоянием, а химводоочистка является важнейшим условием очистки сточных вод котельной. Этот процесс очень важен для оказания положительного влияния на окружающую среду.

По пройденной теме можно сделать следующие выводы:

- химводоочистка – процесс удаления нежелательных химических веществ, биологических загрязнителей, взвешенных твёрдых частиц и газов, загрязняющих пресную воду;
- химводоочистка (ХВО) для котельных предназначена для снижения жесткости воды и ее умягчения, а также очищения воды от вредных примесей;
- химводоочистка является важнейшим фактором очистки сточных вод котельной.

Список использованных источников

1. Инструкция по охране труда для слесаря-ремонтника. - ИОТ ВЧДР-17-076-2016 03.11.2016.
2. Инструкция по охране труда для мастера (старшего мастера). - ИОТ-ВЧДР-17-003-2016 24.06.2016.
3. Инструкция по охране труда для работников, выполняющих уборку рабочих мест территорию депо. - ИОТ-ВЧДР-17-008-2016 21.11.2016.
4. Инструкция по охране труда для оператора котельной. - ИОТ-ВЧДР-17-083-2019 21.06.2019.
5. Инструкция по охране труда для аппаратчика химводоочистки. - ИОТ-ВЧДР-17-082-2019 21.06.2019.
6. Инструкция по использованию средств индивидуальной защиты. - ИОТ-ВЧДР-17-004-2019 30.01.2019.

ОСОБЕННОСТИ ПОДГОТОВКИ КОТЛОАГРЕГАТА К ПУСКУ ИЗ ХОЛОДНОГО СОСТОЯНИЯ

Стурова Евгения Алексеевна, студентка 3-го курса
Научный руководитель Сальков Вадим Анатольевич, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В наше время экологическая обстановка во всём мире постепенно ухудшается, и одна из основных проблем - это котельные установки, являющиеся лидерами по количеству вредных выбросов в окружающую среду и по их ядовитому воздействию.

Вследствие разогрева котельного оборудования из холодного состояния затрачивается большое количество топлива и энергии, соответственно, это вредит атмосфере: увеличивается количество продуктов сгорания, других отравляющих веществ, которые выбрасываются в атмосферу (двуокись серы, соединения ванадия, летучая зола), зависит от состава топлива и его не горючей части.

Такой вид выбросов актуален для больших ТЭЦ, работающих на обогрев города.

При изучении видов топлива установлено, что самым экологичным топливом является природный газ, при его сгорании выделяется наименьшее количество вредных веществ, чем мазута или других видов топлива.

Поэтому необходимо использовать более качественное очистное оборудование. Одним из методов проведение очистки - организация качественной очистки дымохода от золы и установка современных фильтров. Обязательным элементом любой современной котельной являются золоуловители, которые должны очищать исходящий от установки дым на 90%, как минимум.

В ходе изучения предмета исследования сформулировано следующее заключение, что при сжигании различных видов топлива выделяется большое количество углекислого газа, последствия которого приводят к парниковому эффекту. Важной задачей котельных является минимизировать количество выбросов вредных веществ путем установки более качественных и современных очистных сооружений.

Окислы азота NO_x Оксид (NO) и диоксид (NO_2) азота образуются при сгорании топлива при очень высоких температурах (выше 650° С) и избытке кислорода. В дальнейшем в атмосфере оксид азота окисляется до газообразного диоксида красно-бурого цвета, который хорошо заметен в атмосфере большинства крупных городов. Основными источниками диоксида азота в городах являются выхлопные газы автомобилей и выбросы теплоэлектростанций. Кроме того, диоксид азота образуется при сжигании твердых отходов, так как этот процесс происходит при высоких температурах горения. Также NO_2 играет не последнюю роль при образовании фотохимического смога в приземном слое атмосферы. В значительных концентрациях диоксид азота имеет резкий сладковатый запах. В отличие от сернистого ангидрида, он раздражает нижний отдел дыхательной системы, особенно легочную ткань, ухудшая тем самым состояние людей, страдающих астмой, хроническими бронхитами и эмфиземой легких.

При растворении окислов азота в воде образуются кислоты, которые являются одной из главных причин выпадения так называемых «кислых» дождей, приводящих к гибели лесов. Образование в приземном слое озона также является одним из следствий наличия в нем окислов азота. В стратосфере закись азота инициирует цепочку реакций, приводящих к разрушению озонового слоя, защищающего нас от воздействия ультрафиолетового излучения Солнца.

Следовательно, считаю необходимым, использование очистных и фильтрующих сооружений в котельных и цехах, где происходит большое количество сжигания топлива.

Список использованных источников

1. Инструкция по охране труда для слесаря-ремонтника. - ИОТ ВЧДР-17-076-2016 03.11.2016.
2. Инструкция по охране труда для мастера (старшего мастера). - ИОТ-ВЧДР-17-003-2016 24.06.2016.
3. Инструкция по охране труда для работников, выполняющих уборку рабочих мест территорию депо. - ИОТ-ВЧДР-17-008-2016 21.11.2016.
4. Инструкция по охране труда для оператора котельной. - ИОТ-ВЧДР-17-083-2019 21.06.2019.
5. Инструкция по охране труда для аппаратчика химводоочистки. - ИОТ-ВЧДР-17-082-2019 21.06.2019.
6. Инструкция по использованию средств индивидуальной защиты. - ИОТ-ВЧДР-17-004-2019 30.01.2019.
7. Инструкция по оказанию первой помощи пострадавшим. - ИОТ-ВЧДР-17-011-2019 03.12.2019.
8. Инструкция по охране труда при нахождении на железнодорожных путях. - ИОТ-ВЧДР-17-046-2019 30.01.2019.

ТЕПЛООБМЕННЫЕ АППАРАТЫ, ПРИМЕНЯЕМЫЕ В ПРОМЫШЛЕННЫХ КОТЕЛЬНЫХ

Юдина Валерия Александровна, студентка 4-го курса
Научный руководитель Канайчева Ольга Васильевна,
преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Теплообменник не является самостоятельным устройством, но это один из важнейших элементов любой системы теплоснабжения. С каждым годом данные аппараты совершенствуются – уменьшаются их размер и масса, но увеличивается коэффициент полезного действия.

Кожухотрубный теплообменник – это бестопочный сосуд, работа которого основана на явлениях теплообмена и термодинамических процессов между различными жидкостями и газами, причем возможно изменение их агрегатного состояния.

Кожухотрубный теплообменник состоит из пучков труб, трубного и межтрубного пространства, решеток. Нагреваемая среда проходит по трубкам, а горячая - в межтрубном пространстве.

Основной недостаток – это достаточно большие размеры. Иногда крупные габариты служат причиной отказа от использования агрегата. Из этого следует и второй недостаток – большая металлоемкость, которая выливается в высокую стоимость теплообменника. К тому же они довольно «капризные» устройства, рано или поздно потребуется ремонт. Наиболее слабой частью является трубная система, именно в тонких трубках чаще всего выявляется причина поломок.

Пластинчатый теплообменник (ПТО) – это элемент теплоснабжения, передающий тепло от источника к холодной среде с помощью теплопередающей стенки (в этой роли выступают гофрированные пластины), без смешивания жидкостей.

Конструктивно разборный пластинчатый теплообменник, состоит из рамы и пакета пластин.

Рама состоит из неподвижной плиты и прижимной плиты, задней стойки которая соединена с неподвижной плитой верхней направляющей и нижней направляющей. Рамы разборных теплообменников выпускаются разной длины для обеспечения установки в нее разного количества пластин.

Между неподвижной и прижимной плитами находится расчетное количество пластин с резиновыми уплотнительными прокладками.

Пакет прижат к неподвижной плите прижимной плитой стяжными шпильками. Степень сжатия достаточна для уплотнения и герметизации внутренних полостей теплообменника

Пластинчатый теплообменник рассчитывается и должен работать на турбулентном режиме. В этом и заключается его отличие и более высокая эффективность чем у кожухотрубного теплообменника, где течение жидкости ламинарное.

Пластины разборного пластинчатого теплообменника устанавливаются одна за другой с поворотом на 180 град. Эта компоновка создает теплообменный пакет с четырьмя коллекторами для подвода и отвода жидкостей. Первая и последняя пластины не участвуют в процессе теплообмена, задняя пластина выполняется обычно без портов.

В первую очередь следует отметить такое важное достоинство, как простота обслуживания. В тех случаях, когда происходит засорение данного агрегата, необходимо разобрать устройство и тщательно промыть пластины от накипи. После этого его следует просушить и собрать. При этом для данной процедуры не потребуются какие-то большие физические или временные затраты.

Второе преимущество связано с тем, что при использовании данного типа теплообменника можно наблюдать низкий уровень загрязняемости поверхности теплообмена. Это достигается за счёт высокой турбулентности потока жидкости, которая образуется рифлением. Кроме того, на данный фактор влияет также и то, что теплообменные пластины имеют качественную полировку.

Третье важное достоинство заключается в экономичности. Данный агрегат способен прослужить более 20 лет. При этом если в процессе потребуется провести замену пластин, то это легко можно сделать. Так, например, при ремонте кожухотрубного агрегата это затратно.

Поскольку речь зашла о пластинах, следует также сказать о том, что теплосьем такого типа теплообменника в любой момент можно увеличить или уменьшить. Всё, что для этого требуется, - только добавить нужное количество пластин или, наоборот, убрать их. Это также является весьма существенным преимуществом такого рода оборудования.

Учитывая все перечисленные достоинства и недостатки двух видов теплообменного оборудования, можно с уверенностью сказать: экономически выгодные, надежные и эффективные – пластинчатые разборные теплообменники.

Список использованных источников

1. Лариков Н.Н. Теплотехника. - М.: Стройиздат, 1985. - 432 с.
2. Бродов, Ю.М. Справочник по теплообменным аппаратам паротурбинных установок. / Ю.М. Бродов. - М.: ИД МЭИ, 2008. - 480 с.
3. Быков, Л.В. Основы вычислительного теплообмена и гидродинамики / Л.В. Быков, А.М. Молчанов, Д.С. Янышев. - М.: Ленанд, 2019. - 200 с.

Секция 1.3

О ПРОБЛЕМЕ ПРОФИЛАКТИКИ ЭКСТРЕМИЗМА В МОЛОДЕЖНОЙ СРЕДЕ

Бочарникова Надежда Алексадровна, студентка 2-го курса
Научный руководитель Козлова Лариса Михайловна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В настоящее время современное общество ставит перед собой такую задачу как снижение роста проявлений молодежного экстремизма и терроризма, а так же повышение эффективности их профилактики в студенческой среде.

В профилактике нуждается все население, в особенности люди, входящие в группы повышенного риска: дети, подростки, молодежь, а так же люди, ведущие асоциальный образ жизни. Профилактика является одним из перспективных и важных направлений деятельности по преодолению экстремизма и терроризма.

Молодежь – элемент наиболее чувствительный ко всем социальным и политическим изменениям. Она остро реагирует на то, что ей кажется несправедливым, на то, что не совпадает с ее общим мнением, зачастую навязанным псевдогероями из социальных сетей, просторов Интернета.

Основным действующим актом, вокруг которого сформировано всероссийское антиэкстремистское законодательство, является федеральный закон от 25.07.2002 № 114-ФЗ «О противодействии экстремистской деятельности». Как механизм защиты и профилактики, регулирования и пресечения экстремизма закон имеет определенные недостатки: введя понятие «экстремизм», закон не раскрывает сущность данного социального явления, а лишь перечисляет его формы [3].

Профилактика противодействия экстремизму упоминается в законе, в ст.2 и 5, лишь вскользь, меры противодействия экстремизму не конкретизируются, не определены субъекты профилактики.

Как уже было сказано, молодежь в силу своих возрастных, психологических и социальных характеристик всегда острее и активнее реагирует на перемены в обществе. Под влиянием социальных, политических, экономических и иных факторов в молодежной среде, не имеющей прочных идеологических установок, формируются радикальные взгляды и убеждения.

Исследователи проблемы выделяют факторы, способствующие экстремистским проявлениям в молодежной среде [3]:

1. Обострение социальной напряженности в молодежной среде. Экстремизм постоянно подпитывается неопределенностью положения молодого человека и его неустановившимися взглядами на происходящее.

2. Криминализация ряда сфер общественной жизни (широкое вовлечение молодых людей в криминальные сферы бизнеса). Экстремизм возникает и развивается чаще в тех обществах и группах, где отсутствуют самоуважение и уверенность в себе или же условия существования способствуют игнорированию прав личности.

3. Изменение ценностных ориентаций (значительную опасность представляют зарубежные и религиозные организации и секты, насаждающие религиозный фанатизм и экстремизм, отрицание норм и конституционных обязанностей, а также чуждые российскому обществу ценности).

4. Использование в деструктивных целях психологического фактора (агрессия, свойственная молодежной психологии, активно используется опытными лидерами экстремистских организаций для осуществления акций экстремистской направленности).

Молодой человек озабочен желанием найти свою группу, поиском собственной идентичности, которая формируется по примитивной схеме «мы - они». Его психика неустойчива, он легко подвергается внушению и манипулированию.

5. Использование Интернета в противоправных целях (обеспечивает радикальным общественным организациям доступ к широкой аудитории и пропаганде своей деятельности, возможность размещения подробной информации о своих целях и задачах, времени и месте встреч, планируемых акциях) и др.

Наиболее опасным периодом для вхождения в поле экстремистской активности является подростковый и юношеский возраст. На это время приходится развитие самосознания, максимализма, обострение чувства справедливости, определение смысла и ценности жизни. Неудачные попытки найти смысл жизни, неуверенность в себе, ведут к желанию сформировать круг близких по духу людей, найти ответственного за все свои беды и неудачи.

Таким образом, экстремизм в молодежной среде можно рассматривать как неадекватный способ разрешения социально-политических противоречий некоторой части молодежи в области классовых, межэтнических, религиозных и иных социальных отношений соответствующими субъектами последних.

Профилактика молодежного экстремизма становится основным методом борьбы с распространением идеологии экстремизма, так как только воспитательные, пропагандистские меры, направленные на предупреждение экстремистской деятельности, способны дать наилучшие результаты.

В рамках профилактики экстремизма Т.А. Юмашева предлагает использовать следующие формы работы [8]:

– проведение индивидуальных бесед;
– организация факультативных занятий;
– организация встреч с психологами;
– проведение тренингов, круглых столов, экскурсий, тематических вечеров, спортивные мероприятия и др.;
– разработку внутриведомственной статистики, отражающей характер и состояние молодежных девиаций;
– включение во внутриведомственную статистическую отчетность различных учреждений, осуществляющих коррекцию, социальную реабилитацию, медико-психолого-педагогическую поддержку, охрану и защиту детей и семей «группы риска»;
– обеспечение доступности статистической информации о детско-подростковой девиации для всех субъектов образования и воспитания;
– регулярный анализ состояния подростковой безнадзорности и ее последствии;
– оценка эффективности системы профилактики;
– прогнозирование качественного и количественного развития всех компонентов системы;
– своевременное выявление неблагополучных семей, информирование о них центров социальной помощи семье и детству, комиссий по делам несовершеннолетних, выявление несовершеннолетних, нуждающихся в социальной профилактике и реабилитации.

Организация работы по профилактике экстремизма в образовательной организации, как и любая профилактическая работа в колледже, должна начинаться с анализа исходной ситуации. Для этого проводятся социологическое исследование, анкетирование, интервьюирование и другие способы опроса учащихся, родителей и педагогов.

Реализация программ профилактики экстремизма требует достаточно высокого уровня подготовки всех субъектов, а также умения и готовности адаптировать планы и программы с учетом быстро изменяющихся условий жизнедеятельности учащихся, местных и групповых особенностей.

Список использованных источников

1. Методические материалы по профилактике экстремизма в молодежной среде. Вып. 2 / авт.-сост. И.С. Фомин. - Великий Новгород, 2015. - 34 с.
2. Найда А.А. Практические аспекты применения закона о противодействии экстремистской деятельности. Религиозный экстремизм // Практика применения закона о противодействии экстремистской деятельности: сб. матер. науч.-практ. конф. - М., 2016. - С.6-13.
3. Профилактика экстремизма, национализма и укрепление межнациональных и межкультурных отношений в условиях работы образовательных организаций общего образования: метод.рек. [Электронный ресурс] / [сост. Т.А. Ичеткина]; Мин-во образования Респ. Коми, Коми респ. ин-т развития образования. - Сыктывкар: КРИРО, 2015. - 104 с.
4. Профилактика экстремизма в молодежной среде. Проблемы и решения. -Иркутск, 2016. - 105 с.

КОМПЛЕКСНЫЕ СПОСОБЫ ЗАЩИТЫ РАБОТНИКОВ МЕТАЛЛУРГИЧЕСКИХ ПРЕДПРИЯТИЙ ОТ НЕГАТИВНЫХ ПРОИЗВОДСТВЕННЫХ ФАКТОРОВ

Васильева Дарья Алексеевна, студентка 4-го курса
Научные руководители Береговенко Елена Николаевна, преподаватель высшей категории, Цымлянская Валерия Сергеевна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Освоение специальностей, востребованных на металлургических предприятиях, сопряжено с обязательным изучением негативного воздействия факторов производственной среды на каждого работника. При этом разнообразие последствий этого воздействия предполагает внедрение широкого спектра организационных и технических мероприятий. Начиная с видов инструктажей: вводного, первичного и повторного на рабочем месте, внепланового, целевого; и заканчивая автоматическими системами слежения за безопасностью выполнения отдельных технологических операций[1].

Учитывая тот факт, что современное металлургическое производство позиционирует себя как высокоэффективное, с максимальной степенью защиты работников, нам видится интересным поиск универсальных способов, подходящих для сохранения здоровья различных категорий работников.

Цель исследования состояла в анализе сходного воздействия негативных производственных факторов и предложении комплексных способов защиты работников.

Объектом исследования был выбран Оскольский электрометаллургический комбинат.

Предметом исследования – технологические операции основных цехов предприятия.

Основными называют цеха предприятия, выпускающие товарную продукцию. На Оскольском электрометаллургическом комбинате в настоящее время к такой категории можно отнести шесть цехов (таб.1).

Таблица 1 – Продукция основных цехов [2]

<table>
<tr><td rowspan="2">Область воздействия факторов</td><td rowspan="2">Индивидуальные средства защиты</td><td colspan="2">Способы защиты работников</td></tr>
<tr><td>организационные</td><td>технические</td></tr>
<tr><td>Органы зрения</td><td>Очки, маски, шлемы</td><td rowspan="4">Обучение безопасным приемам выполнения трудовых действий
Стажировка на рабочем месте
Проверка знаний по охране труда и комплексной безопасности</td><td rowspan="4">Ограждения, изоляция, удаленное размещение, средства сигнализации и защитного отключения</td></tr>
<tr><td>Органы слуха</td><td>Беруши, наушники, шлемы</td></tr>
<tr><td>Органы дыхания</td><td>Маски, респираторы, противогазы</td></tr>
<tr><td>Кожные покровы</td><td>Спецодежда, спецобувь, перчатки (рукавицы), маски, шлемы</td></tr>
</table>

Каждый цех насчитывает от нескольких сотен до тысячи рабочих мест, параметры которых должны обеспечивать сохранение жизни и здоровья работника в процессе выполнения трудовых функций.

Рассмотрим основные негативные производственные факторы металлургического предприятия. Обычно их подразделяют на две категории: вредные (способные нанести вред здоровью работника при длительном воздействии); опасные (травмирующие).

К первой категории относят: шум, вибрацию, запыленность, загазованность, тепловое излучение. Эти факторы присутствуют на каждом технологическом переделе. Шум

различной интенсивности и частоты оказывает на организм человека неблагоприятное воздействие и может вызвать различного рода болезненные состояния, в том числе тугоухость и глухоту. Источниками шума в цехах являются, главным образом, системы транспортировки сырья и материалов, вращающиеся части электроприводов. Для снижения шума в цехах предусмотрены звукоизолирующие кожухи, шумопоглотители и предусмотрена звукоизоляция служебных помещений и постов управления. Вибрацию порождают неуравновешенные силовые воздействия, возникающие при работе машин. Для ослабления вибрации все агрегаты, создающие ее (двигатели, вентиляторы, рабочие машины), устанавливают на самостоятельных фундаментах, виброизолированных от пола и других конструкций зданий. В качестве средств индивидуальной защиты от вибрации используют рукавицы с двойным слоем: резиновые (снаружи) и хлопчатобумажные (внутри) и виброгасящую обувь. Запыленность воздуха рабочей зоны затрудняет дыхательный процесс, способствует накоплению в тканях организма частиц твердых веществ. Источниками образования пыли служат процессы измельчения и транспортировки сырья и материалов. Снижение концентрации пыли в воздухе рабочей зоны обеспечивается изоляцией рабочих мест, созданием многослойных пылеулавливающих устройств. Индивидуальными средствами защиты работников служат маски, респираторы, очки, наушники, шлемы. Тепловое (инфракрасное) излучение сопровождает не только термические процессы, но и процессы обработки, транспортировки нагретого металла[3]

Ко второй категории относят, прежде всего, воздействие электрического тока, движущиеся части машин и механизмов, работы, выполняемые на высоте. Однако, при определенной интенсивности, травмирующим может оказаться любой вредный фактор (шум ≥ 100 Дб; раскаленный металл; содержание токсичных веществ в воздухе и т.п.). Таким образом, и способы защиты работников тоже могут быть универсальными (комплексными).

В результате исследования, нам удалось сгруппировать отдельные факторы по областям негативного воздействия и описать внедрение комплексных способов защиты работников. В таблице 2 предложены способы защиты работников от воздействия пыли.

Таблица 2 – Комплексные способы защиты работников

<table>
<tr><td rowspan="2">Область воздействия факторов</td><td rowspan="2">Индивидуальные средства защиты</td><td colspan="2">Способы защиты работников</td></tr>
<tr><td>организационные</td><td>технические</td></tr>
<tr><td>Органы зрения</td><td>Очки, маски, шлемы</td><td rowspan="4">Обучение безопасным приемам выполнения трудовых действий
Стажировка на рабочем месте
Проверка знаний по охране труда и комплексной безопасности</td><td rowspan="4">Ограждения, изоляция, удаленное размещение, средства сигнализации и защитного отключения</td></tr>
<tr><td>Органы слуха</td><td>Беруши, наушники, шлемы</td></tr>
<tr><td>Органы дыхания</td><td>Маски, респираторы, противогазы</td></tr>
<tr><td>Кожные покровы</td><td>Спецодежда, спецобувь, перчатки (рукавицы), маски, шлемы</td></tr>
</table>

Важность выявления комплексных (универсальных) способов защиты работников определяет эффективность их применения. Для металлургических предприятий аспект охраны труда имеет первостепенное значение, определяя возможности их развития и конкурентные преимущества в производственной сфере.

Список использованных источников

13. Анализ потенциально опасных и вредных факторов. URL: https://www.studbooks.net (дата обращения: 28.03.2021).

14. Основные производства ОЭМК им. А.А. Угарова // Металлоинвест. Металлургический сегмент. URL: https://www.metalloinvest.com (дата обращения: 28.03.2021).
15. Комплексная защита работников. URL: https://prom-nadzor.ru (дата обращения: 28.03.2021).

АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ УЧЕТА И МОНИТОРИНГА ПРОДУКЦИИ ПРЕДПРИЯТИЯ

Демахин Данила Сергеевич, Цвентарных Владимир Алексеевич,
студенты 1-го курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Аннотация: В данной статье рассматривается проблема учета и мониторинга плодово-ягодных культур. В настоящее время большинство предприятий для ведения учета используют специализированные программы, такие как 1С. Но, как привило, они не учитывают специфику каждого предприятия, а предоставляют набор универсальных средств, которые позволяют полностью автоматизировать бизнес-процессы предприятия.

Ключевые слова: база данных, информационная система, СУБД.

Актуальность разработки информационной системы заключается в повышении эффективности процесса оформления и продажи продукции.

Целью научно-исследовательской работы является проектирование информационной системы учета и мониторинга плодово-ягодных культур на предприятии.

Для достижения поставленной цели необходимо выполнить следующие задачи:

- сформулировать цель разработки информационной системы;
- собрать данные для анализа использования и функционирования ИС;
- провести анализ предметной области;
- построить инфологическую модель данных;
- на основании разработанной ИЛМ создать базу данных в среде выбранной СУБД;
- разработать алгоритмы работы программы;
- разработать эргономичный пользовательский интерфейс;
- разработать справочную систему;
- проанализировать возможные способы обеспечения информационной безопасности данных системы;
- оценить ИС с точки зрения возможностей ее дальнейшего развития;
- выполнить демонстрацию разработанной ИС в соответствии с заданием с целью проверки соответствия результатов работ.

Входная информация представляет собой информацию, поступающая извне и использующаяся как первичная информация для реализации экономических и управленческих функций и задач [3].

Входной информацией разрабатываемой системы являются:

- данные о продуктах предприятия;
- данные о клиентах, взаимодействующих с предприятием.

Выходная информация - это полученная информация на основе входной информации. Выходная информация включает данные предметной области, полученные в результате автоматизированной обработки [3].

Выходными данными являются:

- отчеты;
- статистические данные, позволяющие визуализировать наиболее важные параметры рассматриваемой предметной области.

Перед началом проектирования информационной системы необходимо разработать базу данных, в которой будет храниться необходимая информация в виде двумерных таблиц. База данных будет реализована посредством реляционной СУБД, которые предназначены

для управления, создания и поддержания баз данных. В данной работе была выбрана СУБД Microsoft SQL Server 2016. Microsoft SQL Server обладает всеми качествами, необходимыми для реализации ключевых требований к СУБД, предъявленными заказчиком, а именно – производительностью, стабильностью и возможностью масштабирования. Microsoft SQL Server имеет бесплатный выпуск – SQL Server Express для разработчиков и независимых поставщиков [1].

Достоинства:

- обеспечивает интеграцию с Microsoft Office;
- гарантирует повышенную безопасность;
- гарантирует производительность средств разработки;
- содержит более мощные инструменты бизнес - аналитики.

Информационная система была разработана в среде программирования Microsoft Visual Studio.

Microsoft Visual Studio представляет собой интегрированную среду разработки различных классов приложений для операционной системы Windows, а также имеется возможность создания приложений для ОС Linux, Mac OS и мобильных операционных систем [1].

В ходе проектирования информационной системы был разработан графический интерфейс посредством экранных форм.

Так на рисунке 1 представлена форма нового заказа.

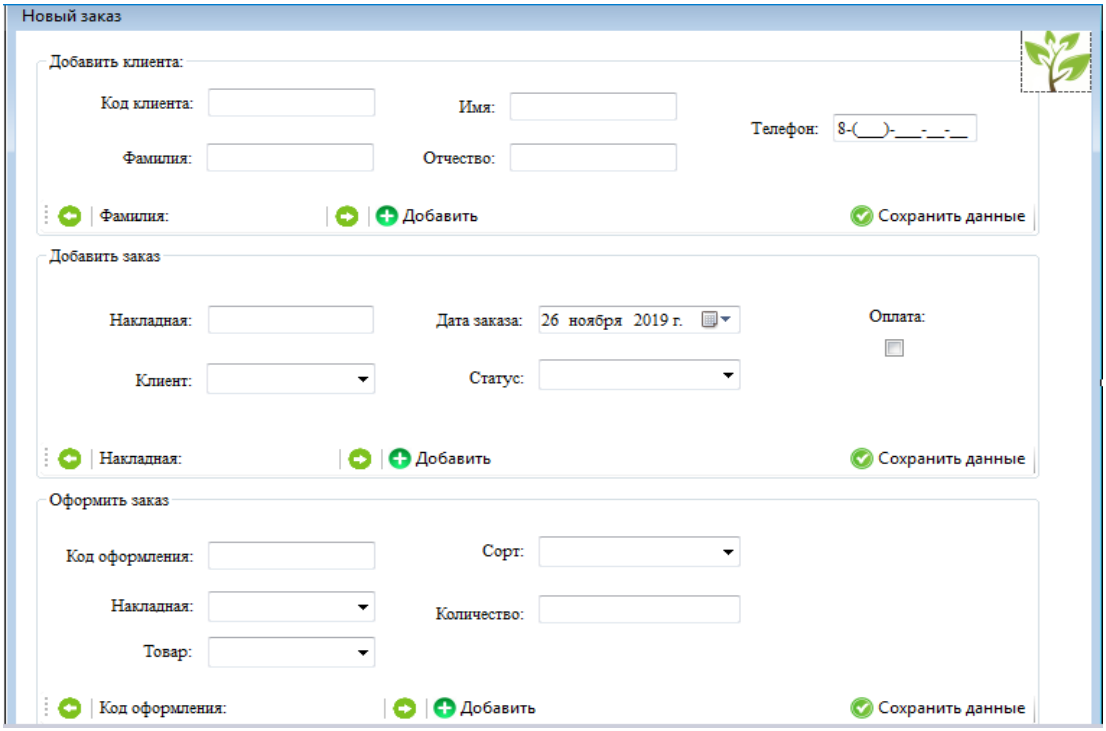


Рисунок 1 - Форма оформления нового заказа

На форме размещены следующие компоненты:

1 – Group Box;

2 – Picture Box.

На рисунке 2 представлена форма мониторинга. На протяжении сезона графики отображают прибыль, а также имеется возможность отследить спрос на каждую категорию продукции.

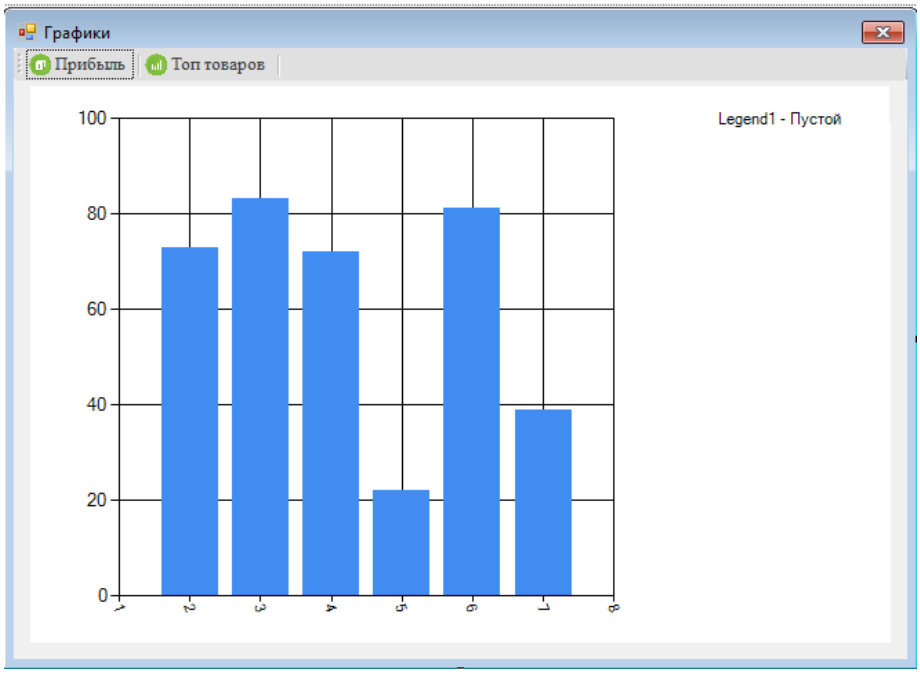


Рисунок 2- Форма мониторинга

Для обеспечения информационной безопасности были приняты следующие меры:

- установлены антивирусные программы;
- настроен брандмауэр;
- обеспечено разграничение доступа к данным в клиентском приложении;

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие/ А.В. Васильков, И.А. Васильков. - М: ФОРУМ: ИНФА-М,2017. - 384 с.

2. Конова Е.А., Поллак Г.А. Язык С++: Учебное пособие. - 4-е изд, стер. - СПб.: Издательство «Лань», 2019. - 384 с.

3. Немцова Т.И. Программирование на языке высокого уровня программирование на языке С++: учебное пособие.

4. Сайт для программистов С#:

[Электронный ресурс]. - http://www.programmerlib.ru/csharp.php

5. Агарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. -324 с.:ил.

МОДЕРНИЗАЦИЯ СИСТЕМЫ АВТОМАТИЗАЦИИ ПОЖАРОТУШЕНИЯ ООО «СПЕЦ-МОНТАЖ ЭЛЕКТРОННЫЕ ТЕХНОЛОГИИ»

Дубовик Сергей Андреевич, студент 4-го курса
Научный руководитель Хархота Надежда Васильевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Под системой охранно-пожарной сигнализации следует понимать целый комплекс технических устройств, которые способствуют своевременному обнаружению, обработке и передаче поступившего сигнала о начале возгорания, нарушения доступа в помещении, подаче определенных команд на включение оповещения людей о пожаре, вызов охраны на место взлома, а также обеспечения срабатывания противодымной защиты, противопожарных клапанов и других устройств, необходимых для комплексного обеспечения безопасности на объекте. Охранно-пожарная сигнализация – это базовый элемент в системе безопасности любого объекта.

Активное внедрение средств пожарной автоматики на объектах позволяет сохранить жизни многим людям и спасти от уничтожения огнем имущество предприятий.[1]

Целью исследования является модернизация системы пожарной сигнализации, системы оповещения людей о пожаре, системы охранной сигнализации и системы контроля и управления доступом, также разработке автоматизации пожаротушения.

Задачи исследования:

- предоставить общие сведения о ООО «Спец-монтаж электронные технологии» и краткую характеристику технологического процесса системы автоматизации пожаротушения;
- описать технологические параметры системы автоматизации пожаротушения;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления;

Объектом является Пожарно-спасательная часть № 46 села Шаталовка.

Система автоматического пожаротушения (АПТ) – это совокупность стационарных технических средств для тушения пожара за счет выпуска огнетушащего вещества.

Основные задачи системы АПТ – обнаружение, локализация и тушение очага возгорания на ранней стадии.

Наиболее эффективны системы автоматического пожаротушения, которые осуществляют:

- постоянный контроль температуры (или наличия дыма) в охраняемом помещении;
- контроль целостности цепей управления, оповещения, питания;
- выдачу сигнала «Тревога» на пульт централизованного наблюдения;
- включение звуковых и световых оповещателей;
- закрытие огнезадерживающих клапанов;
- включение системы дымоудаления на путях эвакуации людей;
- подачу огнетушащего вещества (ОВ);
- оповещение о факте подачи ОВ.[2]

Обоснование характеристик систем обнаружения пожара, оповещения и управления эвакуацией людей при пожаре выполнено в соответствие с требованиями п. 5 ст. 17 Федерального закона от 30 декабря 2009 года № 384-ФЗ «Технический регламент о безопасности зданий и сооружений».[5]

Управление насосами насосной станции пожаротушения осуществляется в ручном режиме.

Включение насосов пожаротушения выполняется от АРМ диспетчера, расположенного в помещении диспетчерская в здании пожарного депо, либо от кнопок дистанционного пуска и по месту.

Кнопки дистанционного пуска устанавливаются на высоте 1,5 м от уровня земли или уровня пола. Конструкция кнопок дистанционного пуска предусматривает защиту от случайного приведения их в действие или механического повреждения.

Объем автоматизации насосной станции пожаротушения:

- сигнализация на АРМ диспетчера состояния насосов (включен, выключен);
- сигнализация на АРМ диспетчера максимального давления в напорном трубопроводе подачи воды на пожаротушение;
- сигнализация на АРМ диспетчера минимального давления в напорном трубопроводе подачи воды на пожаротушение;
- дистанционное и местное измерение давления в напорном трубопроводе;
- дистанционное и местное измерение расхода воды в напорном водопроводе;
- сигнализация на АРМ диспетчера аварийного уровня воды в машинном зале.[3]

Недостатки существующей системы автоматизации является:

-управление насосами насосной станции пожаротушения осуществляется в ручном режиме;

-отсутствует система оповещения оператора о ходе технологического процесса;

-технические средства автоматизации морально и физически устарели.

Для управления системой наружного водяного пожаротушения необходимо установить программируемый логический контроллер (ПЛК).

Автоматизированная система управления пожаротушением позволит производить:

- дистанционный пуск установки водяного пожаротушения;
- автоматический контроль давления в напорном трубопроводе;
- автоматическое включение резервного насоса при остановке основного насоса (АВР);
- автоматический контроль расхода воды в напорном водопроводе;
- автоматическое открытие/закрытие электроприводной запорной арматуры;
- автоматический контроль уровня в резервуарах противопожарного запаса воды;
- автоматический контроль расхода воды в напорном водопроводе;
- автоматическое открытие/закрытие электроприводной запорной арматуры;
- автоматический контроль уровня в резервуарах противопожарного запаса воды;
- автоматический контроль напряжения в цепях управления;
- автоматическое переключение цепей питания с основного ввода электроснабжения на резервный, при исчезновении напряжения на основном вводе, с последующим переключением на основной ввод электроснабжения, при восстановлении напряжения на нем;
- световая и звуковая сигнализация;
- об аварийном и минимальном уровне воды в резервуарах противопожарного запаса воды;

Установить световые указатели мест установки соединительных головок для подключения передвижной пожарной техники. Данные световые указатели включаются автоматически при включении установки пожаротушения и пожарной сигнализации.

- аварийное включение резервного насоса при останове рабочего, сигнализация оператору;
- контроль на обрыв и короткое замыкание соединительных линий дистанционного пуска установки пожаротушения, световых оповещателей, исполнительных устройств;
- пуск насосов пожаротушения от кнопок:

1. у насосной станции пожаротушения;
2. у резервуаров противопожарного запаса воды РГСН;

3. у пожарных гидрантов ГПН-1 на территории пожарного депо;
4. у пожарных кранов в здании пожарного депо;

Для резервуаров противопожарного запаса воды РГСН-100 и РГСН-50 автоматизация необходимо предусмотреть в следующем объеме:

- сигнализация на АРМ диспетчера и по месту (световая и звуковая) аварийного уровня в резервуаре, закрытие задвижки ЭП1, отключение работающего насоса, установленного в насосной станции пожаротушения;
- сигнализация на АРМ диспетчера аварийного уровня в резервуаре;
- сигнализация на АРМ диспетчера и по месту минимального уровня в резервуаре, открытие задвижки ЭП1, включение насоса, установленного в насосной пожаротушения;
- сигнализация на АРМ диспетчера состояния электроприводной задвижки (авария, закрыта, открыта);
- контроль на обрыв и короткое замыкание соединительных линий от световых и звуковых оповещателей, исполнительных устройств;

Для визуализации технологического процесса в аварийных режимах работы предусмотрена сенсорная панель, расположенная на двери шкафа АПТ.

Для исследования динамики системы в приложении Simulink разработана математическая модель насосной установки, позволяющая проводить моделирование с учетом и без учета ограничений регулятора давления и с возможностью подачи на вход системы задания различного вида. Схема модели САУ насосной установки приведена на рисунке 1.

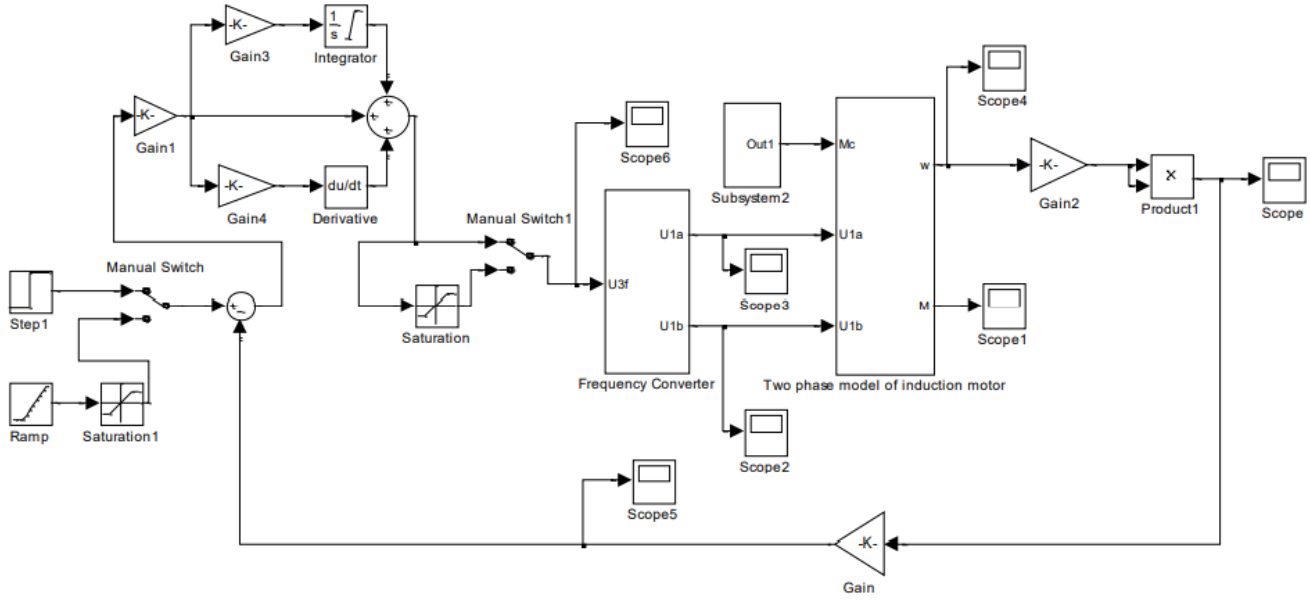


Рисунок 1 -Математическая модель контура регулирования воды в насосной установки

Для решения поставленных задач необходимо:

- выбрать панели оператора- сенсорная C-movemicrographicC-moreMicro-Graphic. Панель оператора 4" TFT с сенсорным экраном 320 x 240, дисплей 32 768 цветов со светодиодной лампой подсветки. 5 функциональных клавиш со светодиодными индикаторами. Два встроенных порта - USB и RS-232/422/485. Дисплей поддерживает альбомный и портретный режимы;
- контроллер modiconquantumПЛК для систем автоматизации промышленных процессов;
- датчики давления Метран-150-TG;
- преобразователи расхода вихреакустические Метран-300 ПР;

- пост кнопочный серии ПОК;
- датчик контроля протечки воды SW 005;
- АРМ диспетчера, в состав АРМ диспетчера входят:
- сервер базы данных реального времени для хранения производственной и технологической информации.
- программная среда (SCADA) для разработки, управления, контроля и поддержки промышленных приложений, визуализации процессов, интеграции различных промышленных систем управления и диспетчеризации в единую систему управления.
- средство проведения анализа данных, представления отчётной документации, графической информации.
- набор инструментов для разработки, создания, тестирования и развертывания промышленных приложений автоматизации.
- единая среда разработки, отладки приложений и операционная среда для контроллеров.

Таким образом, разработанная система предусматривает возможность предоставления обслуживающему персоналу в реальном масштабе времени всей необходимой информации для принятия решений по управлению технологическим процессом пожаротушения. Модернизацией предусмотрено подключение основных параметров контроля и управления к контроллеру АСУ ТП, обеспечивающему сбор, предварительную обработку и передачу информации от датчиков полевого уровня автоматизации на АРМ диспетчера. Согласно заложенным проектным решениям, существует возможность регистрации всех необходимых параметров и формирования сигнализации в диспетчерской. Результатом модернизации явилось создание комплекта проектной документации, удовлетворяющей действующим требованиям стандартов, разработанной по заданию проектной организации ООО «Спецмонтаж электронные технологии».

Список использованных источников

1. Бабуров В.П., Бабурин В.В., Фомин В.И., Смирнов В.И. Производственная и пожарная автоматика. Ч.2. Автоматические установки пожаротушения: Учебник. М.: Академия ГПС МЧС России, 2007. - 298 с.
2. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.
3. Микрюков В.Ю. Безопасность жизнедеятельности: учебник / В.Ю. Микрюков. - 10-е изд., перераб. и доп. – Москва : КНОРУС, 2019. – 282 с.
16. СП 5.13130.2009. Системы противопожарной защиты. Установки пожарной сигнализации и пожаротушения автоматические. Нормы и правила проектирования. - Введ. 2009-03-25- М.: МЧС России, 107 с.
17. СП 3.13130.2009 «Системы противопожарной защиты. Система оповещения и управления эвакуацией людей при пожаре. Требования пожарной безопасности».

СВЯЗАННЫЕ ОДНОЙ СЕТЬЮ: ВЗГЛЯД СТУДЕНТОВ НА ДИСТАНЦИОННОЕ ОБУЧЕНИЕ

Жаркова Екатерина Алексеевна, студентка 2-го курса
Научный руководитель Козлова Лариса Михайловна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Говоря о дистанционном обучении, в первую очередь следует понимать, что его появление не является внезапным событием, во все времена потребность в образовании сохранялась на высоком уровне, а с появлением интернета и ускорением темпов научного прогресса, данный запрос приобретает всё большие масштабы, из чего следует, что появление дистанционного обучения - это не банальный ответ на кризисные события, а новый, полноценный способ получения образования, который получил дополнительное ускорение в развитии за счёт внешних факторов.

В статье рассматриваются некоторые аспекты отношения студентов к дистанционному формату, исходя из полученного опыта. На основе данных опроса студентов металлургического отделения ОПК СТИ НИТУ «МИСиС», анализируется их представление о возможном месте дистанционного обучения в будущем и готовность уже в ближайшее время сделать выбор в пользу данной формы обучения.

Мы опросили студентов 2 и 3 курсов специальностей ОМД, МЧМ и ТТО о переходе на удаленный формат и различных аспектах дистанционного обучения. Было опрошено 124 студента. Опрос проводился при помощи Google Forms .

В целом, студенты удовлетворены условиями дистанционного обучения и отлично или хорошо адаптировались к новым условиям (73,4 %). Более того, к совмещению традиционных занятий в колледже и онлайн обучению положительно относятся более 85% опрошенных.

Работа преподавательского состава в рамках дистанционного обучения оценивается студентами положительно (67%). Студенты отмечают, что большинство преподавателей всегда на связи (64,5%). И если в прошлом учебном году большинство преподавателей использовали при обучении платформу Canvas, то сейчас абсолютное большинство за комбинацию Microsoft Teams + Canvas. Студенты отмечают только положительные моменты от данного перехода (65, 4% опрошенных).

Если рассматривать уровень самооценки навыков пользования компьютером, только 4% студентов декларируют, что не имеют навыков работы с ПК. Большинство респондентов (66%) являются обычными пользователями ПК на самом элементарном уровне, т.е. используют компьютер в своей учебной деятельности в качестве «печатной машинки».

Если говорить о плюсах дистанционного обучения, то среди наиболее явных - отсутствие необходимости выезжать в учебное заведение (65,1%) и возможность для обучающихся участвовать в организации своего учебного процесса: выбирать время и место для работы с учебным материалом, определять скорость изучения материала, соответствующую особенностям своего мышления (22,2%).

Важным отличием дистанционной модели от традиционной является развитие личностных качеств обучаемого, в частности его способности к непрерывному образованию и самообразованию, что соответствует реализации одной из тенденций современного образования. Однако результаты анкетирования показали, что на практике студенты не рассчитывают на собственные силы. Оказалось, что на самостоятельное решение поставленной задачи надеются только 37% опрошенных. В связи с этим следует подчеркнуть, что при организации обучения с использованием дистанционных технологий важную функцию выполняет самоконтроль, так как основную часть учебной нагрузки обучаемый должен выполнять самостоятельно. Среди опрошенных 54% пытаются

осуществлять самоконтроль. Но, к сожалению, эти попытки не всегда доходят до конечного результата. Очень часто возникают психологические проблемы, которые студент преодолеть не может, т.е. ему необходим дополнительный стимул «со стороны», выраженный либо в назидательной форме, либо в «карающей».

Анализируя вопросы, вязанные с возникшими у студентов трудностями, можно сделать вывод, что основными проблемами, с которыми сталкиваются студенты, являются следующие.

- Недостаток живой коммуникации с педагогом и сверстниками, (30,5%).
- Большой объем информации и заданий (22,7%).
- Технические проблемы (отсуствие Интернета, дорогой интернет, плохой компьтер/телефон) (18.7%)
- Отсутствие мотивации к учебной деятельности без постоянного контроля со стороны преподавателя (19,4%).
- Невозможность сравнивать промежуточные результаты своего обучения и других студентов (14,9%).
- Плохая обратная связь (11,3%).
- Проблемы со здоровьем (падает зрение, недостаток движения, болит спина/шея), (17,8%).

Таким образом, в большинстве своем, студенты адаптировались к дистанционному обучению, оценивают работу преподавательского состава колледжа положительно.

В итоге хотелось бы сделать вывод, что в нашем мире разделять людей постоянно просто невозможно. Поэтому перспективы повсеместного дистанционного обучения весьма туманны. Думаю, мы не будем скучать по онлайн-формату обучения. Но этот ценный опыт поможет нашему колледжу координировать студентов вне учебного заведения и какие-то элементы дистанционного обучения навсегда останутся с нами, аккуратно слившись с повседневным учебным распорядком. Мы даже не заметим, когда случится этот симбиоз.

Список использованных источников

1. Чванова М.С., Киселева И.А. Проблемы дистанционного обучения в сети Интернет // Вестник российских университетов. Математика. 2017. № 5-2.
2. Шатуновский В.Л., Шатуновская Е.А. Ещё раз о дистанционном обучении (организация и обеспечение дистанционного обучения) // Вестник науки и образования. 2020. № 9-1 (87).
3. Тихомиров В.П., Солдаткин В.И. Дистанционное обучение: к виртуальным средам знаний [Электронный ресурс] // Научно-практический журнал «Открытое образование». Режим доступа: http://www.e-joe.ru/sod/99/2_99/st158 (дата обращения: 18.03.2020).

СВЕТОДИОДЫ И ИХ ПРИМЕНЕНИЕ

Иваницкий Даниил Антонович, Томилин Никита Геннадиевич,
студенты 1-го курса
Научный руководитель Амельчакова Елена Анатольевна, преподаватель.
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Впервые об излучении света твёрдотельным диодом было сообщено в 1907 году британским экспериментатором Генри Раундом из лаборатории Маркони.

Токопроводимость светоизлучающего диода была аналогична полупроводниковому. В 1923 году руководитель Нижегородской радиотехнической лаборатории, О.В. Лосев заметил голубоватое свечение, испускаемое некоторыми полупроводниковыми детекторами, которые преобразуют высокочастотный сигнал радиостанции в низкочастотный звуковой в простейших радиоприёмниках. Холодный свет рождался внутри карбидокремниевого кристалла вследствие неизвестных тогда электронных превращений. Из наблюдений был сделан вывод, что полупроводниковый кристалл может усиливать и генерировать высокочастотные радиосигналы, сопровождающееся и световым излучением. К концу 2006 года светодиоды стали широко применяться на современном рынке.

Светодиод — полупроводниковый прибор, излучающий некогерентный свет при пропускании через него электрического тока. Работа основана на физическом явлении возникновения светового излучения при прохождении электрического тока через p-n-переход. Цвет свечения определяется типом используемых полупроводниковых материалов.

Виды светодиодов. Индикаторные светодиоды являются наиболее компактным видом и имеют совсем небольшую силу света - до ста мКд. Рабочий диапазон тока составляет около 20 миллиампер. Такой вид выпускается в стандартном корпусе, оснащенном выводами с диаметром основания в три миллиметра, или пять миллиметров. Чаще всего используются в оптических индикаторах. Индикаторные светодиоды для поверхностного монтажа широко применяются в системах отображения информации в качестве основных излучающих элементов, для подсветки жидкокристаллических матриц и др. Основные тенденции их развития - повышение световой эффективности и надежности.

Сверхъяркие светодиоды состоят из полупроводниковых кристаллов малого или среднего размера (до 500 микрометров). Создаваемый световой поток (белый цвет) - до 30 лм, и даже более. Рабочий диапазон тока здесь может составлять до 100 миллиампер. Применяются в сотовых телефонах, рекламных вывесках. Светоотдача мощных светодиодов составляет более 50 лм/Вт. Мощность равна одному ватту. Используется для общего наружного светодиодного освещения.

Моргающие светодиоды практически не отличаются от обычных светодиодов, однако в них используется встроенный кругооборот мультивибратора, что позволяет создавать мерцания светодиода с периодом в секунду. Большинство моргающих светодиодов излучает однотонные световые лучи, но более сложные способны вспыхивать двумя-тремя цветами одновременно, либо поочередно. Применяются в качестве индикатора привлечения внимания.

Разноцветные моргающие светодиоды - это фактически два различных светодиода в одном, работающие навстречу, поэтому при загорании одного, второй гаснет. В одном направлении током производится один цвет, а в противоположном - другой, чередование двух цветов с определенной частотой является причиной появления третьего цвета, смешанного.

Трёхцветные светодиоды - это пара светоизлучающих диодов в одном, но они связаны, чтоб работать отдельно, точнее, чтоб два светодиода одновременно светили и управлялись независимо.

Применение светодиодов.

1. Нелинейная обработка аналоговых сигналов. Диоды применяются в детекторах, логарифматорах, экстрематорах, преобразователях частоты и в других устройствах для нелинейной обработки аналоговых сигналов. В таких случаях диоды используют для обеспечения прохождения главного сигнала, или же в качестве косвенных элементов, например в цепях обратной связи.

2. Выпрямители. Устройства, которые используются для получения постоянного тока из переменного называются выпрямителями. В большинстве случаев они включают в себя три главных элемента – это силовой трансформатор, непосредственно выпрямитель (вентиль) и фильтр для сглаживания. Диоды применяют в качестве вентилей, так как по своим свойствам они отлично подходят для этих целей.

3. Стабилизаторы. Устройства, с помощью которых стабилизируется напряжения на выходе источников питания, называются стабилизаторами. Они бывают разных видов, но каждый из них предполагает применение диодов. Эти элементы могут использоваться либо в цепях, отвечающих за опорные напряжения, либо в цепях, которые служат для коммутации накопительной индуктивности.

4. Ограничители. Ограничители – это устройства, используемые ограничения возможного диапазона колебания различных сигналов. В цепях такого типа широко применяются диоды, которые имеют прекрасные ограничительные свойства.

5. Устройства коммутации. Диоды применяются и устройствах коммутации, которые используются для того, чтобы переключать токи или напряжения. При помощи диодных мостов размыкают или замыкают цепь, которая служит для передачи сигнала. В работе применяется некоторое управляющее напряжение, под воздействием которого и происходит замыкание или размыкание. Иногда управляющим может быть сам входной сигнал, такое бывает в самых простых устройствах.

6. Логические цепи. В логических цепях диоды используют для того, чтобы обеспечить прохождение тока в нужном направлении (элементы «И», «ИЛИ»). Подобные цепи используются в схемах аналогового и аналогово-цифрового типа.

Достоинства:

1. Механическая прочность и надёжность.

2.Высокий уровень электро- и пожаробезопасности обеспечивается отсутствием нагрева и высокого напряжения.

3. Быстродействие благодаря безынерционности.

4. Миниатюрность.

5. Долгий срок службы.

6. Высокий КПД.

7. Низкое энергопотребление.

8. Разнообразие цветов свечения, направленность излучения.

9. Регулируемая интенсивность.

Недостатки:

1. Относительно высокая стоимость.

2. Малый световой поток от одного элемента.

3. Деградация параметров светодиодов со временем.

4. Повышенные требования к питающему источнику.

Список использованных источников

1. С.Л. Бухарин // Методические указания: «Специальные источники света» 2011 г.
2. https://radioelementy-ru.turbopages.org/radioelementy.ru/s/articles/vidi-diodov/
3. https://fb.ru/article/338188/vidyi-diodov-harakteristiki-primenenie

УТИЛИЗАЦИЯ ОТХОДОВ ПРОИЗВОДСТВА ЧЁРНОЙ МЕТАЛЛУРГИИ

Карапузов Роман Анатольевич, студент 3-го курса
Научные руководители Старых Галина Александровна, преподаватель высшей категории, Демба Ирина Михайловна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

На современном этапе в России остро стоит проблема недостатка оборудования для утилизации отходов, особенно промышленных. В Российской Федерации перерабатывается не более 30% отходов, остальное просто закапывают в землю, располагают на свалках, занимающих территории более 130 км². Такое нецелесообразное использование отходов металлургического производства приводит к загрязнению плодородных земель тяжёлыми металлами, попаданию их в реки, озёра, водоёмы и испарению выделяющихся газов в атмосферу.

Металлургия является одним из основных источников загрязнения окружающей среды. Отходы металлургического производства включают в себя все остатки от переработки сырья и к ним необходимо применять качественную утилизацию.

Промышленные отходы черной металлургии в настоящее время широко применяются для вторичной переработки, в результате чего их неблагоприятное влияние на окружающую среду уменьшается. Хронология действий, связанных с обработкой отходов, следующая: предупреждение образования – сокращение образования – повторное использование – окончательное удаление.

В металлургической промышленности уже на стадии добычи руды происходит возникновение отходов производства. При этом следует отметить, что примерно 70% вскрышных пород и отходов обогащения можно использовать при производстве строительных материалов.

Современное производство предлагает большое разнообразие способов утилизации отходов. Рассмотрим некоторые из них.

Обезвоживание технологических осадков технологией Geotube®. Технология Geotube® – это современный экологически чистый способ обезвоживания осадков и шламов. Технологический процесс состоит из гравитационного обезвоживания различных по происхождению суспензий (ил, пульпа, осадок, шлам). Это происходит в тканых контейнерах, которые сшиты из полипропиленового материала на основе ткани марки с достаточно высокой плотностью. Материал по своей сущности имеет уникальную тонкую структуру пор, которая обеспечивает задержку шламовых частиц малого размера в контейнере и не препятствует свободному выходу из него остаточной влаги. Благодаря такой системе работы технология Geotube® обеспечивает высокую производительность без значимых капитальных затрат выходом до 1600 м³ обезвоженного материала в одном контейнере.

Использование технологии Geotube обладает рядом преимуществ: маневренность технологии, отсутствует необходимость капитального строительства, незначительная энергоемкость, технологический процесс непрерывен, существует возможность применения технологии при отсутствии технологической воды, низкие эксплуатационные затраты.

Недостатки: для реализации способа геотуб, необходимо иметь свободное пространство для геотекстильных мешков, водоносную станцию, геотубы не могут быть использованы повторно.

Естественный способ. Обезвоживание шламов производится на специально подготовленных площадках для естественной сушки. Они представляют из себя спланированные, обвалованные земляными валиками участки (карты). Шламы подсыхают

здесь до влажности 7–9%, уменьшаются в объеме от 1,5 до 12 раз, приобретают удобную для транспортировки и использования структуру.

Подсушенный осадок вывозят автомашинами, для чего конструкцией предусмотрен съезд на каждую шламовую площадку и запланированы автомобильные дороги. На небольших площадках довольно часто устраиваются узкоколейные пути для вывоза осадка вагонетками. Загрузка автомашин и в особенности вагонеток обычно производится вручную.

Естественная сушка с дренажем имеет ряд недостатков: чрезмерная длительность сушки, малая степень высушивания, необходимо иметь большие площади для отстойников.

Способ фильтрации. Процесс подготовки влажных шламов к фильтрации довольно трудоемкий. Первый этап обезвоживания металлургических шламов - это сгущение, которое происходит в сгустителях. По сути, сгустители представляют собой отстойники, под действием сил гравитации происходит процесс повышения концентрации сгущаемого продукта. Влажность продукта, после процесса сгущения остается ещё довольно высокой - до40 %.

Вторым этапом, после процесса сгущения, продолжается обезвоживание шлама методом фильтрации через специальную синтетическую ткань на основе полиамидных волокон. Процесс фильтрации проходит либо под разряжением (в вакуум - фильтрах), либо под повышенным давлением (в пресс - фильтрах).

Достоинствами дисковых вакуум-фильтров можно назвать следующее: максимальная площадь фильтрующей поверхности, а, следовательно, и наибольшая производительность; возможность быстрой и простой замены секторов с порванной фильтротканью; низкая металлоемкость. Недостатком вакуум-фильтров является быстрый износ фильтрующей ткани.

Утилизация пыли. Состав выносимой пыли существенно зависит от состава применяемой шихты. Особенно это заметно при производстве стали в дуговых сталеплавильных печах.

Современная металлургическая промышленность использует ряд технологий, которые перерабатывают сталеплавильные пыли, такие как:

- переработка плавильной пыли, содержащей цинк и свинец;
- переработка пыли, содержащей хром и никель;
- переработка пыли при ее нагреве в вакууме;
- использование методов гидрометаллургии;
- производство стекла.

Утилизация окалины. Существует два пути утилизации окалины: возврат ее в металлургическое производство или использование ее в других производствах (например, в лакокрасочном).

Проблема утилизации замасленной окалины в настоящее время состоит из двух этапов: сначала её обезмасливают, получая чистую обезжиренную окалину, которая затем легко утилизируется.

Проанализировав патентную проработку, становится определённо понятно, что биологический метод утилизации отходов активно используется в промышленности и непрерывно проводится работа над его совершенствованием. Техническим результатом является упрощение технологии получения органоминеральных удобрений для сельского хозяйства в процессе промышленной утилизации шламов металлургического производства.

Переработку извлеченного из отвала шлака на фракции выполняют путем размола с удалением агломератов металла, который затем отправляют на переплавку. Шлак промывают водой на сите, впоследствии дробят в роторной дробилке и совершают разделение на фракции с получением шлакового песка.

Суть биологического метода очистки заключается в получении коммерчески рентабельного продукта для широкого использования в качестве биоминерального удобрения в сельском хозяйстве. Например, использование раствора шлама металлургического производства в качестве комплекса органоминеральных добавок в

культивационной среде при проращивании семян кукурузы позволяет увеличить массу вегетативной части 7-дневных проростков кукурузы более чем на 60% по сравнению с контрольным образцом, не содержащим добавок.

Экспериментальные данные подтвердили возможность использования биологической утилизации шламов металлургического производства. Эти шламы, которые содержат тяжелые металлы, можно активно применять в качестве биоминерального комплекса стимуляции роста высших растений.

Но есть и проблема: этот метод утилизации ещё мало используется, так как технология новая и находится на стадии разработки и потенциального внедрения, а не всеобщего использования и полноценной информации о его полном процессе пока нет. Но уже имеются достаточное количество данных по применению биологического метода утилизации шламов.

Список использованных источников

1. Отходы металлургического производства [Электронный ресурс] // Musorish. URL: https://musorish.ru/othody-metallurgicheskogo-proizvodstva/ (дата обращения: 18.03.2021).
2. Малашенкова А.В. Усовершенствование технологии подготовки и утилизации замасленной окалины прокатного производства [Электронный ресурс] // Магистр ДонНТУ. URL: http://masters.donntu.org/2006/fizmet/malashenkova/diss/index.htm (дата обращения: 18.03.2021).
3. Утилизация отходов металлургии [Электронный ресурс] // Портал магистров ДонНТУ. URL: http://masters.donntu.org/2007/mech/pozhidaev/library/9.htm (дата обращения: 18.03.2021).
4. Кузнецов Д.В., Близнюков А.С. Способ утилизации шламов металлургического производства [Электронный ресурс] // FindPatent.RU. Дата добавления: 2015.05.2010. URL: https://findpatent.ru/patent/255/2550652.html (дата обращения: 18.03.2021).
5. Виды и классификация металлургических отходов [Электронный ресурс] // emchezgia.ru. URL: http://emchezgia.ru/ekologiya/1_Vidy_otkhodov.php (дата обращения: 18.03.2021).
6. Скрипченко В.В., Тимофеева А.С., Короткова Л.Н. СПОСОБЫ УТИЛИЗАЦИИ МЕТАЛЛУРГИЧЕСКОГО ШЛАМА [Электронный ресурс] // Студенческий научный форум – 2017. URL: https://scienceforum.ru/2017/article/2017038153 (дата обращения: 18.03.2021).
7. Переработка отходов черной металлургии [Электронный ресурс] // Allbest.ur. Дата добавления: 30.05.2016. URL: https://revolution.allbest.ru/manufacture/00685472_0.html (дата обращения: 18.03.2021).
8. Е.П. Большина. Экология металлургического производства [Электронный ресурс] // Кафедра металлургических технологий. URL: http://nf.misis.ru/download/mt/ekology_metallurg_proizvodstva.pdf (дата обращения: 18.03.2021).
9. Влияние металлургической промышленности на окружающую среду и здоровье человека. Меры по снижению воздействия [Электронный ресурс] // Greenologia. URL: https://greenologia.ru/eko-problemy/metallurgicheskay-promyshlennost.html (дата обращения: 18.03.2021).
10. Воздействие металлургических предприятий на окружающую среду [Электронный ресурс] // Allbest.ur. Дата добавления: 27.10.2015. URL: https://knowledge.allbest.ru/ecology/3c0b65635a3ad69b5d53a89521216c36_0.html (дата обращения: 18.03.2021).

АНАЛИЗ ПОТЕНЦИАЛЬНЫХ ОПАСНЫХ И ВРЕДНЫХ ФАКТОРОВ СТАЛЕПЛАВИЛЬНОГО ПРОИЗВОДСТВА ОЭМК И ОХРАНА ОКРУЖАЮЩЕЙ СРЕДЫ

Каськов Андрей Александрович, студент 3-го курса
Научные руководители Старых Галина Александровна, преподаватель высшей категории, Демба Ирина Михайловна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Металлургическое производство характеризуется непрерывностью технологических и трудовых операций и работы механизмов и машин. В этих условиях опасные и вредные производственные факторы проявляют себя постоянно. Цель моего исследования - проанализировать опасные и вредные факторы в металлургическом производстве и оценить меры принятые по созданию безопасных условий труда.

Опасные производственные факторы в электросталеплавильном цехе

Электросталеплавильный цех - в печном пролете основную опасность представляют неорганизованные выделения вредностей от электропечей: тепловыделения; шум от электрических дуг; выбивание из печи газов, содержащих пыль, окись углерода, окислы азота и серы, цианиды, фториды, пары хрома, никеля, марганца; пылевыделения при ремонтах печи. Окислы азота выделяют в атмосферу пролета также печи для нагрева ферросплавов. В печном пролете предусматривают естественную аэрацию, установку вентиляторов на рабочей площадке, отсос печных газов через отверстие в своде и иногда с помощью зонтов, устанавливаемых над печью. Отсос газов с помощью зонтов менее эффективен, чем через отверстие в своде. Количество вредных выбросов можно сократить, если при отсосе печных газов поддерживать под сводом давление, равное атмосферному; при этом исключается подсос воздуха в печь и в отводимых и выбивающихся газах будут отсутствовать окислы азота и цианиды. Для новых цехов рекомендуется сооружение вокруг печи кожуха, который изолирует цех от шума и обеспечивает улавливание вредностей, выделяющихся при плавке и выпуске стали; отводимые из кожуха газы подвергают очистке. Другим вариантом локализации выделения вредностей является сооружение между печным и смежными пролетами разделительных стенок. Этот способ менее эффективен, так как не защищает от вредностей персонал печного пролета.

Вредные производственные факторы в электросталеплавильном цехе

Вредные факторы производственного процесса при длительном и интенсивном их воздействии на человека могут привести к возникновению профессиональных заболеваний трудящегося. К этим факторам относятся:

а) тепловые, ультрафиолетовые, ионизирующие и другие излучения;

б) электромагнитные поля;

в) яркое слепящее световое излучение;

г) выделяющиеся в атмосферу производственного помещения пыль и газ;

д) высокий уровень шума и вибрации, ультразвук.

Рабочие ЭСПЦ подвергаются воздействию всех вышеперечисленных факторов.

Работодатель обязан сделать все возможное, чтобы снизить отрицательное воздействие сложившихся производственных факторов на свой персонал. Это делается путем повышения степени автоматизации производства, оптимизации характера рабочих обязанностей, предоставления защитных средств и другими способами. Однако если в результате применения всех этих мер привести класс условий труда работников к оптимальному или хотя бы допустимому не удается, работодатель обязан будет предоставить сотрудникам, которые вынуждены работать в таких условиях, установленные

законом льготы и компенсации. Определение класса условий труда осуществляется в ходе отдельной процедуры – спецоценки (СОУТ).

ОАО «ОЭМК» является современным металлургическим предприятием. При производстве стали применена технология, основанная на прямом восстановлении железа с использованием природного газа, что позволяет получать металл с минимальным негативным воздействием на окружающую среду. В проекте ОАО «ОЭМК» реализованы передовые технологические решения по охране атмосферного воздуха.

Применение системы гидротранспорта для поставки железорудного концентрата исключает использование железнодорожного транспорта, операций погрузки и разгрузки. Процесс бесшумен, легко поддается контролю, регулированию и автоматизации, беспылен.

Использование для межцеховых и внутрицеховых транспортировок сырьевых и производственных материалов закрытых конвейерных систем и специального автотранспорта позволяет исключить загрязнение окружающей среды за счет исключения запыленности при транспортировке сырья.

Все основные технологические агрегаты обеспечены пылегазоочистыми установками. В настоящее время в подразделениях ОАО «ОЭМК» эксплуатируется 97 пылегазоочистных устройств. Существующее пылегазоочистное оборудование обеспечивает эффективность очистки от пыли в пределах 90-99%.

Очистка газов от пыли, в основном, сухая – электрофильтры (10 шт.), тканевые фильтры (53 шт.), циклоны (14 шт.) и только с целью снижения пожароопасности пыли, за некоторыми системами предусмотрена установка мокрых систем очистки газов – скруббера (20 шт.) (на системах транспортировки металлизованных окатышей в ЦОиМ, ЭСПЦ). Ряд установок имеют двухступенчатые очистки: пылевая камера и электрофильтр (за вращающимися печами ЦОИ); циклон и электрофильтр, (мельница, сушильный барабан бентонита в ЦОиМ), циклон и тканевый фильтр (шлифовальные станки в ЭСПЦ, шлифовальные машины в СПЦ-1), батарейный циклон и мокрый скруббер (участок шихтоподачи в ЭСПЦ).

Важнейшей целью в области природоохранной деятельности комбината является снижение и предотвращение отрицательного воздействия на окружающую среду в процессе производственной деятельности, обеспечение необходимой защиты здоровья и безопасности работников комбината и в близлежащих населенных пунктах. Для этого в бюджете предприятия в 2012 году на охрану окружающей среды было инвестировано 1560,424 млн. руб., в том числе на модернизацию газоочистки ДСП-150 №1-4 было затрачено 965,088 млн. руб. из них на завершение работ по первому модулю - 908,109 млн. руб.

На протяжении ряда лет выбросы загрязняющих веществ в атмосферный воздух оставались на комбинате приблизительно на одном уровне – 45 888т – 46 921т. Разница по валовым выбросам по годам колеблется от 0,22% до 2,25% и зависела в основном от выпуска продукции. Но модернизация газоочистки печей ДСП-150 №3,4 (модуль №1) привела к снижению выбросов твердых компонентов и СО, так как конструктивные особенности установки позволяют дожигать СО и снижать температуру дымовых газов при перемещении по газоходам.

Вследствие этого, выбросы вредных веществ по ОАО «ОЭМК» в 1 полугодии 2013 года составили 14863,957т, что на 8211,071 т (35,58%) ниже уровня выбросов за 1 первое полугодие прошлого года.

Удельные выбросы загрязняющих веществ на 1 т выпущенной стали в 1 полугодии в 2010 и 2012 года оставались практически на одном уровне, 14 кг на 1 тонну выплавленной стали, но в 1 полугодии 2013 произошло заметное снижение – 9 кг на 1 тонну.

В своей работе ОАО «ОЭМК» руководствуется принципом неукоснительного выполнения требований законодательства Российской Федерации, международных стандартов, норм и правил в области охраны окружающей среды.

На комбинате разработан проект нормативов предельно допустимых выбросов (ПДВ), получено разрешение на выброс загрязняющих веществ в атмосферный воздух.

ОАО «ОЭМК» постоянно осуществляет систематический производственный контроль за выбросами загрязняющих веществ в атмосферу и эффективностью работы пылегазоочистных сооружений, в соответствии с графиками аналитического контроля технологических выбросов и атмосферного воздуха от основных источников ОАО «ОЭМК» и графика проверки эффективности работы пылегазоочистных сооружений. Пылеочистные установки работают эффективно. Выбросы загрязняющих веществ не превышают норматив ПДВ.

Еженедельно, в соответствии с утвержденным графиком контроля, отбираются пробы воздуха на территории комбината, на границе СЗЗ, в близлежащих населенных пунктах, а также дополнительно производится отбор проб атмосферного воздуха в городе, в парке кинотеатра «Быль».

При выполнении замеров максимально разовые концентрации примесей не превысили ПДК для населенных мест и в среднем в 2012 составили от 6 до 60%ПДК м.р.

На территории комбината запыленность атмосферного воздуха в среднем на уровне ПДК для населенных мест, а концентрации газообразных загрязняющих веществ существенно (в 2 и более раз) ниже ПДК для населенных мест.

По результатам наблюдений на границе СЗЗ ни по одному из загрязняющих компонентов, выбрасываемых в атмосферный воздух, превышения ПДК м.р. не было установлено.

Проанализировав опасные и вредные факторы в металлургическом производстве и оценив меры, принятые по созданию безопасных условий труда делаю вывод, что при проектировании ОЭМК были предусмотрены новейшие технологии и в настоящее время комбинат является наиболее современным высокоавтоматизированным и высокопроизводительным предприятием в России и Европе с высокой мерой защиты от воздействия опасных и вредных факторов.

Список использованных источников

1. Современные подходы при проектировании и строительстве металлургических заводов последнего поколения.URL: https://musorish.ru/othody-metallurgicheskogo-proizvodstva/ (дата обращения: 18.03.2021).
2. Правовые аспекты проблем охраны природы в металлургии. URL: http://emchezgia.ru/ekologiya/22_Pravovye_aspekty_problem_okhrany_prirody.php МЧ-ЗГИА.РУ ©. (дата обращения: 18.03.2021).
3. Организация работы в сталеплавильном цехе. URL: http://emchezgia.ru/ekologiya/30.2_Osobennosti_organizatsii_raboty.php МЧ-ЗГИА.РУ ©. (дата обращения: 18.03.2021).

РЕШЕНИЕ ТЕХНОЛОГИЧЕСКИХ ЭКОЛОГИЧЕСКИХ И СОЦИАЛЬНЫХ ПРОБЛЕМ С ПОМОЩЬЮ РАЗЛИЧНЫХ МЕТОДОВ ТВОРЧЕСКОЙ ДЕЯТЕЛЬНОСТИ

Кирпита Артём Олегович, студент 3-го курса
Научные руководители Старых Галина Александровна, преподаватель высшей категории, Козлова Лариса Михайловна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Студенты ОПК СТИ НИТУ «МИСиС» активно участвуют в конфекциях и чемпионатах на различных уровнях. В 2019-2020 г. студенты металлургического отделения ОПК приняли участие в международном чемпионате METAL CUP и заняли 5 и 7 места. Для решения кейсовых заданий студенты применяли методы для решения проблемных задач.

В 2020-2021 г. студенты МО ОПК пробуют свои силы кейс-чемпионате «РазРеши», в связи с чем стал вопрос о более емком изучении данных методов.

Целью данной статьи является изучение методов творческой деятельности и выявление оптимальных путей решения кейсов.

Задачи:

- рассмотреть методы решения технологических, экологических и социальных задач;
- рассмотреть эффективность различных методов решения;
- выявить и обосновать самый действенный метод;
- применить данный метод на решении задач.

Гипотезой исследования выступает утверждение о том, что освоение и применение различных методик творческой деятельности должны помочь в решении конкретных технологических задач.

Кажется, мы все знаем, что такое проблемы и как их решать. Если нет стандартных решений, мы ищем варианты, перебираем их. Применяем так называемый метод проб и ошибок. И иногда много уходит впустую – где-то дни, где-то годы. Как найти оптимальный выход из сложившейся ситуации? Как организовать поиск решений, чтобы не повторять ошибки? Этим вопросам посвятил долгие годы изучения Генрих Саулович Альтшулер. Он проделал огромную работу по изучению нескольких тысяч патентов на изобретения и выявил определенные закономерности в решении изобретательских задач. Альтшулер установил, что все инженерные и технические системы развиваются по определенным законам, зная которые, можно находить решение проблем. Эти принципы он положил в основу созданной им теории ТРИЗ – теории решения изобретательских задач. Те или иные принципы, впервые сформулированные в ТРИЗ, используются во всех современных методиках достижения успеха. Теория решения изобретательских задач – совокупность методов решения технических задач и усовершенствования технических систем.

Основу ТРИЗ составляют 40 общих приёмов создания изобретений и 76 стандартных шаблонов решений. Для решения конкретной задачи пользователи ТРИЗ сводят её к концептуальной части и пытаются применить подходящий общий метод, а позднее вернуться к конкретной задаче.

Участники международного чемпионата METAL CUP, команда «Осколсталь», при решении кейса по разработке технологических решений «Повышение эффективности переработки вышедших из эксплуатации автомобилей» использовали алгоритм Альтшулера. По мнению капитана команды, в кейсах, вне зависимости от уровня и лиги, всегда есть задачи, которые обычными размышлениями не решить, и как раз в этом деле помогает алгоритм Альтшуллера. Он позволяет найти различные нестандартные решения, а это - то, что нужно на чемпионате.

Надо заметить, что все инструменты ТРИЗ работают не вместо мышления, а для мышления. То есть, они не заменяют собой человека, а помогают в решении творческих, инженерных и технических задач.

Таким образом, использование методов технического творчества дает возможность для старта мотивированных студентов в практико-ориентированные занятия в сфере науки, техники и технологий. Такие занятия должны формировать навыки труда и практической деятельности, включая элементы профориентации в научно-техническую сферу.

Участие в различных чемпионатах студентов Оскольского политехнического колледжа – яркое тому подтверждение. Используя при решении кейсов методы «Диаграмма Иссикава», Smart, ранжирование и алгоритмы ТРИЗ можно решить практически любую проблему. А дальше - яркое представление, уверенность в своих силах, и, как итог, победа над собой и конкурентами.

Список использованных источников

1. Алгоритм решения изобретательских задач для профессионалов. - Тель-Авив, 2003. - 286 с. Утёмов В. В. Приемы разрешения противоречий в научном творчестве // Концепт. - 2013. - № 04 (апрель). - ART 13078. -URL: http://e-koncept.ru/2013/13078.htm (дата обращения: 18.03.2021).
2. Альтшуллер Г. С. Найти идею. - Новосибирск: Наука, 1991. - 225 с.
3. Зиновкина М. М., Утёмов В. В. Структура креативного урока по развитию творческой личности учащихся в педагогической системе НфТм-ТРИЗ // Концепт. - 2013. - Современные научные исследования. Выпуск 1. - ART 53572. - URL: http://e-koncept.ru/2013/53572.htm (дата обращения: 18.03.2021).
4. Певзнер Л. Х., Рыбникова Т. А. Азбука изобретательства. - Екатеринбург: Среднеуральское книжн. изд-во, 1992. - 240 с.

ПРАВОВАЯ ПОДДЕРЖКА ПРОФСОЮЗА В РОССИЙСКОЙ ФЕДЕРАЦИИ

Колесникова Ангелина Сергеевна, студентка 4-го курса
Научный руководитель Макаренок Ольга Николаевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Профсоюзы - явление не новое ни в России, ни в мире. Именно профсоюзы представляют собой те организационные образования, которые могут оказать работникам конкретного предприятия необходимую правовую поддержку в процессе разрешения споров, которые могут возникнуть между предприятием и работником.

Роль профсоюза *актуальна* в экономической и социальной жизни России. Сегодня профсоюзы - единственная сила в России, представляющая интересы самых широких слоев населения. В настоящее время реализация права на защиту прав работников является большой *проблемой*.

Чтобы решить эту проблему, я изучила следующие *задачи*:

- изучение истории возникновения и развития профсоюзного движения в капиталистических странах;
- изучение правовых основ положения профсоюзной организации в Российской Федерации;
- анализ проблем в сфере труда Российской Федерации;
- проведение социологического опроса среди студентов 4 курса на тему «Защита трудовых прав работника в настоящее время»;
- разработка практических рекомендаций для молодых специалистов в области труда.

Изучив историю возникновения и развития профсоюзного движения в капиталистических странах, можно проследить сложный путь реализации прав трудящихся, так как первая реакция работодателей на появление рабочих объединений была отрицательной. Для борьбы с ними вводились специальные законы, запрещающие рабочие союзы и вводящие уголовную ответственность за членство в «заговорщицких организациях».

Не смотря на все это в 70 – 80 гг. различные схемы защиты профсоюзов уже можно было встретить во всех регионах мира, как в развитых, так и в развивающихся странах. Сегодня можно утверждать, что основные цели международного профсоюзного движения достигнуты - профсоюзы пользуются широкими правами, работникам гарантирована минимальная заработная плата, 8-часовой рабочий день и 40-часовая рабочая неделя. [1]

Изучив теоретические и правовые основы положения профсоюзов в Российской Федерации, следует подчеркнуть, что по сравнению с Западом российские профсоюзы с самого начала имели свои особенности. Если в странах Западной Европы и США профсоюзы возникли в эпоху домонополистического капитализма и до создания политических партий, то массовые профсоюзы в России возникли в обстановке революционного подъема, в результате трансформации отвергнутых правительством экономических требований в политические. В России, как и в других странах мира, профсоюзы стали первой формой организации, наиболее доступной широкой общественности. [2]

Проанализировав проблемы в сфере труда Российской Федерации, такие как: множественность, нечеткость и неопределенность функций, неоднородность социального состава, в результате чего учитываются не все обстоятельства. Разные категории работников имеют соответственно разные интересы, отсутствие реальных ощутимых результатов, клише и стереотипы, сложившиеся в течение многих лет, низкий профессионализм и недостаточная компетентность профсоюзных работников.

Можно с уверенностью отметить, что эти факторы отрицательно влияют на имидж профсоюзов в целом, а также отдельных профессиональных организаций и их членов, и в

силу этого широкие массы работающего населения не доверяют профсоюзным организациям и поэтому не хотят участвовать в их деятельности, вступать в ряды профсоюза.[3]

В ходе проведения социологического опроса среди студентов 4 курса на тему "Защита трудовых прав работника в настоящее время" были заданы следующие вопросы:

1) Какие способы защиты трудовых прав вы знаете?

2) Знаете ли вы, что такое профсоюз?

3) Каковы основные функции и задачи профсоюза?

4) С какой целью вы вступите в профсоюзы?

Было опрошено 130 студентов выпускных групп, результаты этого опроса показали неудовлетворительную ситуацию. Молодые специалисты даже понятия не имеют о профсоюзе и профсоюзах, 30% опрошенных имеют представление об этой организации, но они не знают, с какой целью вступают в профсоюз.

Такая ситуация в правовой безграмотности работником не приведёт в будущем к прогрессу в нашем государстве. В связи с этим мной разработаны рекомендациями для молодых специалистов, которые необходимо доносить и разъяснять во время учебного и воспитательного процесса.

Рекомендации «Профсоюз и работник».

1) Углубить профессиональные и теоретические знания о профсоюзе и профсоюзных организациях на рабочем месте, для этого можно прочитать: Трудовой Кодекс Российской Федерации статья 370. "Право профсоюзов осуществлять контроль за соблюдением трудового законодательства и иных нормативных правовых актов, содержащих нормы трудового права, выполнением условий коллективных договоров и соглашений."

2) Участвовать в работе по вовлечению молодежи в активную профсоюзную деятельность.

Список использованных источников

1. Диденко Т.А. История зарубежных стран/ статья:
Режим доступа: https://pandia.ru/text/80/381/43908.php

2. Тютюков А.А.Образование профсоюзного движения в России/статья: Режим доступа:https://star-union.ru/istoriya-profsoyuznogo-dvizheniya-v-rossii/

3. Профсоюзы в современной России. Проблемы профсоюзов/Учебный материал.: Режим доступа:https://studwood.ru/809466/pravo/profsoyuzy_sovremennoy_rossii

АНАЛИТИЧЕСКИЙ КОНТРОЛЬ ПРОИЗВОДСТВА

Косарев Сергей Игоревич, студент 4-го курса
Научный руководитель Котельникова Марина Павловна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Необходимым условием успешной работы предприятия является контроль показателей качества на всех этапах производства: от анализа сырья до поставки продукции потребителю. Только такой контроль может обеспечить эффективность управления производственными процессами и необходимую ритмичность производства. Полная и достоверная информация о качестве продукции формируется по результатам аналитического контроля. Оперативное и надежное управление такой информацией является одной из основных функций службы аналитического контроля. Аналитическая служба является формой организации аналитического контроля в промышленности. [1]

Аналитический контроль — это деятельность, связанная с определением химического состава, структуры и свойств веществ и материалов (объектов аналитического контроля) с последующей оценкой соответствия объекта установленным требованиям. Процедура аналитического контроля включает в себя операции отбора и подготовки пробы (образца), идентификацию, определение состава, структуры и свойств, оценку соответствия установленным требованиям. [2]

Роль контроля металлургического производства невозможно переоценить, т. к. металлы и сплавы, материалы черной и цветной металлургии, играют важную роль в машиностроении, электротехнике, электронике и многих других отраслях. Качество этих материалов в значительной степени зависит от характера и содержания примесей, а свойства сплавов определяются специально вводимыми легирующими добавками. Задачи анализа металлов и сплавов многообразны: определение примесей и легирующих добавок, определение газообразующих примесей, фазовый и локальный анализ. Иногда необходимо определить не только общее содержание компонентов в пробе, но и их распределение по площади или глубине. При анализе металлов и сплавов большое практическое значение имеет атомно-эмиссионный метод, позволяющий проводить многоэлементный анализ (позволяет более 70-ти элементов одновременно). Нашли свое применение атомно-абсорбционный, фотометрический, электрохимический методы анализа. Для определения так называемых газообразующих примесей применяют плавление в вакууме, активационный анализ, масс-спектрометрию.

Аналитический контроль на металлургическом производстве в настоящее время предусматривает определение до 74 элементов периодической системы Д. И. Менделеева и нескольких сотен фаз, определяющих технологические свойства используемых материалов (руды, концентраты, ферросплавы, огнеупоры, шлаки и т. д.). Существенно возросло не только разнообразие исследуемых в черной металлургии материалов, но и количество образцов, результаты анализа которых имеют решающее значение для управления производственным процессом.

Современные технологии выплавки и внепечной обработки стали характеризуются высокой степенью интенсивности протекающих процессов. В рамках жестких требований по оперативности аналитического контроля технологических процессов экспрессность и точность проведения анализа являются одними из ключевых факторов, определяющих соблюдение регламентируемого технологического цикла и скорости проведения корректирующих воздействий.

Тенденции развития металлургического производства, постоянное повышение требований к качеству выпускаемой продукции определяют основные направления развития аналитического приборостроения для черной металлургии.

Серьезной задачей производственного контроля, особенно экспрессного, является его автоматизация. Развитие аналитического контроля металлургического сырья идет в направлении увеличения многокомпонентности анализа.

Важнейшими методами, используемыми для экспресс-анализа продуктов сталеплавильного и ферросплавного производства, являются квантометрические варианты атомно-эмиссионного и рентгеноспектрального методов анализа. Так, на металлургических комбинатах, где полупродуктами и продуктами являются металлы и сплавы, до 75% анализов проводят спектральными методами на вакуумных и рентгеновских квантометрах и экспресс - анализаторах.

Отобранные из металлургических агрегатов пробы металла или шлака по пневмопочте пересылаются в экспресс-лабораторию за 30—40 секунд, где на участке пробоподготовки они разрезаются и шлифуются со стороны среза. Подготовка проб для спектрального анализа занимает 1,0—1,5 минуты. Затем пробы вводят в многоканальные спектрометры. Определение основных компонентов происходит за 3,0—3,5 минуты. Измеренные аналитические сигналы автоматически пересчитываются в определяемые содержания элементов. Результаты анализа о составе металла и готовности его к выпуску передаются сталевару в среднем через 4—7 минут после отбора пробы из печи. Полученная информация используется в управлении металлургическим процессом.

Экспресс - анализ газообразующих примесей H, C, N, O и S проводят на автоматических газоанализаторах.

В зависимости от объекта аналитического контроля и его цели различают следующие производственные виды анализов, с помощью которых производят оценку химического состава: маркировочные, контрольные, скоростные, арбитражные.

Маркировочные анализы проводят для контроля химического состава и свойств сырья и материалов, поступающих на предприятие. Они предназначены также для объективной оценки работы предприятия. По результатам маркировочных анализов определяют качество полупродуктов и готовой продукции, ее соответствие установленным нормам. Маркировочные анализы должны отличаться большой достоверностью и правильностью, так как на их основе делают технологические и экономические расчеты.

Контрольные анализы проводят при необходимости проверки или уточнения результатов маркировочных анализов с применением тех же методов, но более тщательно и точно. [3]

Скоростные (экспрессные) методы применяют при текущем контроле промежуточных и готовых продуктов, с их помощью устанавливают правильность технологического режима. Основное требование, предъявляемое к анализам этого вида, - повышенная скорость, чтобы результаты могли быть своевременно использованы в процессе производства.

Арбитражные анализы производят в случае необходимости получения особенно точных сведений о химическом составе, при разногласиях между заводом-поставщиком и предприятием-потребителем, например, по поводу химического состава сырья.

При проведении анализов используют химические, физико-химические и физические методы.[4]

Совершенствование методов аналитического контроля способствует повышению качества продукции и достижению большей стабильности технологических процессов. Это совершенствование идет в направлении автоматизации серийных анализов, более широкого использования экспрессных инструментальных методов.

На предприятиях металлургической промышленности аналитический контроль производства осуществляет специальная служба, в которую входят несколько лабораторий. Функции их разнообразны. Они ведут научно-исследовательские и экспериментальные

работы, направленные на использование в производстве современных научно-технических достижений, на обеспечение технического развития предприятия. В их задачи входят лабораторное освоение и проверка работ, выполненных в научно-исследовательских учреждениях, последующее участие в освоении этих работ на производстве, разработка новых, более совершенных методов аналитического контроля сырья, полуфабрикатов, готовой продукции и способов контроля технологических процессов.

Служба аналитического контроля осуществляет оперативное руководство технологическим процессом, контроль качества готовой продукции, технологических выбросов и состояния окружающей среды, а также контроль содержания в исходном сырье и промежуточных продуктах вредных примесей.

Сегодня одна из важнейших задач аналитического контроля производства – это максимальное упрощение анализа, чтобы он стал действительно массовым. Это достигается несколькими путями. Один из них – миниатюризация. Уже появились весьма компактные, портативные спектрометры, есть микрохроматографы, выполненные на основе микроэлектромеханических систем. Развивается подход, получивший название "лаборатория на чипе". В целом, аналитическая химия впитывает все то, что создается в рамках других направлений науки и техники, например, электроники.

Основные требования, предъявляемые к методам контроля и анализа веществ - правильность и хорошая воспроизводимость результатов, низкий предел обнаружения нужных компонентов, избирательность, экспрессность, простота анализа, возможность его автоматизации. В отдельных случаях важна локальность определений, анализ на расстоянии (без непосредственного контакта с анализируемым объектом), анализ без разрушения образца. Для массовых анализов большое значение приобретает фактор экономичности определений. Все эти требования отражают основные тенденции развития современных методов анализа материалов.

Список использованных источников:

1. Аналитическая служба, её цели и особенности. https://studref.com/587655/tehnika/analiticheskaya_sluzhba_tseli_osobennosti

2. Родзевич А.П., Газенаур Е.Г. Методы анализа и контроля веществ: учебное пособие //Юргинский технологический институт. - Томск: Изд-во Томского политехнического университета, 2013. - 312 с.

3. Глубоков, Ю.М. Аналитическая химия: учебник для студ. учреждений сред. проф. образования/ [Ю. М.Глубоков, В.А. Головачёва, Ю.А. Ефимова и др.]; под ред. А.А. Ищенко.- 12-е изд., стер. – М.: Издательский центр «Академия», 2017.– 480 с. ISBN 978-5-4468-5882-8 https://may.alleng.org/d/chem/chem451.htm

4. Аналитический контроль производства https://zinref.ru/000_uchebniki/04400proizvodstvo/000_lekcii_proizvodstvo_01/105.htm

АКТУАЛЬНОСТЬ ШТРИХОВОГО КОДИРОВАНИЯ, КАК ЗАЛОГ БЕЗОПАСНОЙ ПРОДУКЦИИ

Куликов Иван Олегович, Сотникова Екатерина Игоревна, студенты 2-го курса
Научный руководитель Иванова Анастасия Игоревна,
преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В последние десятилетия во многих странах, в том числе и в России, является внедрение разновидности информационных технологий, основанных на использовании штрихового кодирования (не только в торговле, сфере услуг, но и в промышленном производстве для идентификации печатных плат, сборочных узлов, изделий, упаковок, в почтовых и транспортных ведомствах, банковской системе, клиниках и пр.) по передаче информации с помощью носителя данных – символа штрихового кода.

Штриховым называют код, состоящий из знаков набора параллельных чередующихся темных (штрих) и светлых (пробел) полос различной ширины в соответствии с ГОСТ Р ИСО МЭК16022-2008. Размеры полос стандартизованы. Самый узкий штрих принят за единицу. Каждая цифра (разряд) складывается из двух штрихов и двух пробелов.

Технологии штрихового кодирования весьма эффективно применяют в розничной торговле, что имеет большое значение для потребителей. Наличие штрих-кода на товаре позволяет полностью автоматизировать процесс управления движения товаров от момента их поступления в магазин до продаж покупателю. Любые операции с каждой единицей товара учитываются в центральном компьютере магазина, тем самым обеспечивается автоматический контроль динамики продажи товара, изменение товарных запасов. Такая технология учета позволяет автоматизировать бухгалтерскую деятельность, анализировать итоги работы по структурным подразделениям, что заметно улучшает финансово-коммерческую деятельность торгующей организации, и оперативно удовлетворять нужды потребителей.

Информация в штриховом коде определяется соотношением ширины штрихов и пробелом. Высота не несет информационную нагрузку и выбирается из соображений легкости считывания – она должна обеспечить пересечение лучом сканера всех штрихов кода.

Штриховые коды можно условно разделить на два типа:

- товарные (имеют два ряда – штриховой и цифровой),
- технологические (имеют один ряд – штриховой).

Товарные кода были созданы специально для идентификации производимых товаров, учета их при транспортировке и управления складскими и торговыми процессами.

Штриховой ряд в товарном коде предназначен для оптического считывания путем поперечного сканирования. Сканер декодирует штрихи в цифры через декодер (микропроцессор) и вводит информацию о товаре в компьютер.

Цифровой ряд предназначен потребителю, информацию для которого ограничена только указанием страны и возможностью проверки подлинности штрих-кода по контрольному разряду. Полный штриховой код позволяет закупочным торговым организациям иметь четкие реквизиты происхождения товара и адресовано предъявлять претензии по качеству, безопасности и другим параметрам, не соответствующим контракту договора.

Разработано большое разнообразие товарных штрих - кодов. К ним относят код UPC, применяемый в США и Канаде, и код EAN, созданный в Европе на основе кода UPC и используемый практически на всех континентах.

Контроль штрих-кода необходим для исключения ошибок при вводе в компьютерные системы (особенно это качается кодов большой длины), а также для проверки подлинности штрих - кодов.

Алгоритм расчета контрольной цифры. Этот алгоритм применим для штрих - кодов EAN-8, EAN-13, UPC, ISBN, ISSN. При этом используется один и тот же алгоритм вычислений по модулю 10.

Для расчета контрольной цифры следует пронумеровать все разряды цифрового ряда справа налево, начиная с позиции контрольного разряда (первый).

Затем:

- начиная со второго, сложить цифры всех четных разрядов;
- полученную сумму умножить на 3;
- начиная с третьего, сложить цифры всех нечетных разрядов;
- сложить результаты, полученные во втором и третьем пунктах;
- значение контрольного разряда является наименьшим числом, которое в сумме с величиной, полученной в пункте 4, даст число, кратное 10.

Полное совпадение контрольной цифры с добавляемой для кратности цифрой, означает, что товар произведен законно и его качество гарантируется.

В связи с тенденцией информационных технологий в настоящее время существуют приложения проверки кодов и их расшифровки. Актуальными приложениями являются такие, как:

Считыватель QR-кода PRO

Приложение довольно просто в использовании: достаточно навести камеру на код и он тут же отобразиться. Также присутствует опция «фонарик», ее можно использовать при недостаточном освещении в помещении.

Плюсы: абсолютно бесплатно, высокая скорость считывания, простой и понятный интерфейс, сканирование происходит автоматически.

Минусы: приложение доступно только для операционной системы Android, владельцам «яблочных» устройств придется использовать аналоги.

Молния QR-сканер

Еще одно приложение для считывания кодов, которое обладает широким функционалом и возможностью подсветки в темноте. Работает на операционной системе Android.

Плюсы: простой и понятный интерфейс, почти мгновенное сканирование.

Минусы: некоторые виды QR-кодов не поддерживаются, а также отсутствует возможность установить приложение на IOS.

Сканер QR и штрих-кодов PRO

Создатели этого приложения продумали буквально все: и автоматический сканер тут есть, и подсветка. Приложение очень просто использовать, даже начинающий юзер с легкостью справится.

Плюсы: есть функция, позволяющая сканировать коды для получения скидок в местных супермаркетах, простой и понятный функционал.

Минусы: у этого приложения они не выявлены.

Молния QR Сканер Штрих-код

Важное преимущество: для сканирования не нужно подключаться к сети интернет. Довольно приятный дизайн и широкий функционал с возможностью сканирования 2в1.

Плюсы: опция фонарик; считывает все возможные коды.

Минусы: в приложении огромное количество рекламы, избавиться от которой можно только заплатив за нее.

Сканер QR-кодов и штрих - кодов

Широкий функционал. Возможность делиться информацией с помощью кода.

Плюсы: установить приложение можно с версии Android 4.1.

Минусы: не обнаружено.

Система автоматизированной идентификации товара на много облегчит труд работников занимающимся учетом и продаж товаров, так как нанесение штрихового кода ускоряет процесс идентификации товара.

Расшифровка и подробная информация по штрих-коду помогает избежать контрафактной продукции, что обеспечивает безопасность жизни потребителя. Как видно, существуют несколько способов проверки информации о продукции по штрих-коду, что играет положительную роль и каждый метод имеет свои плюсы. Именно поэтому в последнее время штриховое кодирование стало играть большую роль не только в специфических сферах, но и в нашей повседневной жизни.

Список использованных источников

3. Хрусталёва, З.А. Метрология, стандартизация и сертификация. Практикум/ З.А. Хрусталёва. – М.: КНОРУС, 2017. – 280 с.
4. Штриховое кодирование // Студопедия. URL: https://studopedia.ru/13_172995_shtrihovoe-kodirovanie.html (дата обращения: 28.03.2021)

ПРОБЛЕМА БЕССМЕРТИЯ

Лихушина Олеся Александровна, студентка 3-го курса
Научный руководитель Дембa Ирина Михайловна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Актуальность исследования проблемы смерти обусловлена тем обстоятельством, что в последние годы этой теме уделяется повышенное внимание в философии, религии, искусстве развитых стран. Развивается целая отрасль знания – танатология.

К сожалению, или к счастью, все в этом мире имеет свое начало и свой конец. Конечность жизни, неизбежная смерть определяют трагичность земного существования человека. Поэтому человечество ищет пути и средства продлить жизнь. Издревле человек ставил перед собой вопрос, в чем сущность человеческого бытия. Многие философы и мыслители пытались ответить на вопрос, для чего живет человек, для чего пришел он в этот мир, почему он умирает и что происходит с ним после смерти.

Человек – самое уникальное и противоречивое творение природы и истории. Только люди способны задумываться о смысле жизни и осознавать конечность собственного существования. Проблемы смерти и бессмертия в философии занимают центральное место. Во все времена этот вопрос интересовал пророков, религиозных деятелей, великих мыслителей, педагогов и врачей.

Смысл смерти. В жизни каждого человека может наступить момент, когда смерть будет более действенной для его главных целей, чем жизнь; когда-то, за что он стоит, благодаря его смерти станет более ясным и убедительным, чем если бы он поступил любым другим образом.

Смерть – это совершенно естественное явление, она играла полезную и необходимую роль в ходе длительной биологической эволюции.

Только факт смерти ставит в глубине вопрос о смысле жизни. Жизнь в этом мире имеет смысл именно потому, что есть смерть[4]. Смысл связан с концом. И если бы не было конца, т.е. если бы была дурная бесконечность жизни, то смысла в жизни не было бы. Смерть - предельный ужас и предельное зло - оказывается единственным выходом из дурного времени в вечность, и жизнь бессмертная и вечная оказывается достижимой лишь через смерть.

Бессмертие – это вечное, непрекращающееся существование. С естественно - научной точки зрения, достичь такого состояния невозможно. Тем не менее, рассуждение на эту тему встречалось у всех древних народов.

Проблема бессмертия. Проблема бессмертия - основная, самая главная проблема человеческой жизни, и лишь по поверхности и легкомыслию человек об этом забывает. Иногда он хочет убедить себя, что забыл, не позволяет себе думать о том, что важнее всего.

Учение о перевоплощении еще менее дает бессмертия целостному человеку, оно предполагает его разложение на отдельные элементы и ввержение человека в космический круговорот, оставляет его во власти времени. Человек может перейти в нечеловеческий род существования.

Виды бессмертия: бессмертие в генах, растворение, мумификация тела, Вечность в памяти.

Этические аспекты проблемы жизни и смерти. Современная танатология (учение о смерти) представляет собой одну из “горячих” точек естественнонаучного и гуманитарного знания. Интерес к проблеме смерти обусловлен несколькими причинами.

Почти 1,5 миллиарда жителей планеты живут в полной нищете и еще 1 миллиард приближается к отметке, 1,5 миллиарда землян лишены какой-либо медицинской помощи,

миллиард людей не умеют читать и писать, в мире насчитывается 700 миллионов безработных;

200 миллионов детей вынуждены работать с младенческого возраста, чтобы не умереть с голода. Миллионы людей во всех уголках земного шара страдают от расизма, ксенофобии, агрессивного национализма.

Это приводит к выраженному обесцениванию человеческой жизни, к презрению жизни как своей, так и другого человека. Вакханалия терроризма, рост числа немотивированных убийств и насилия, а также самоубийств – это симптомы глобальной патологии человечества на рубеже XX - XXI в.

Смертная казнь – проблема скорее социально-политическая, нежели биоэтическая. Это понятие применимо к высшей мере наказания за те или иные преступления, устанавливаемой государством.

Смерть – главный инструмент государственной власти, без применения или угрозы которого ее не станут воспринимать всерьёз. Многие века смертная казнь, в том числе в самых жестоких формах, применялась самыми разными государствами и их противниками.

Мечта людей о личном бессмертии родилась в глубине веков. Она имела и религиозно-пессимистические (когда бессмертными считались только боги), и религиозно-оптимистические формы (когда люди верили в вечную загробную жизнь). Но время шло, и вера иссякла. Человек все чаще отрекался от богов, и вот уже являются сонмы не верующих ни в богов, ни в посмертное вечное блаженство. Они жаждут земных радостей, и можно сказать, что борьба с преждевременными смертями, за долгую и счастливую жизнь (если не для себя, то, по крайней мере, для своих потомков) составляет основную цель всего исторического развития человечества. С научной точки зрения бессмертие невозможно, однако наука рассматривает способы увеличения срока жизни человека. По современным оценкам потенциальный срок жизни, ограниченный человеческим геномом составляет порядка двухсот лет, однако реальные условия жизни серьезно его сокращают. Кроме того, рассматриваются варианты продления жизни за счет пересадки и замены органов, «отправки в будущее» посредством заморозки в криогенных камерах, оцифровывания сознания.

Список использованных источников

1. Филиппова Л.А. Проблема смерти и бессмертия в философии - смысл жизни и взгляды философов [Электронный ресурс] // Наука. Club. URL: https://nauka.club/filosofiya/problema-smerti-i-bessmertiya.html (дата обращения: 29.03.2021).
2. Проблема смерти и бессмертия личности [Электронный ресурс] // Справочник от Автор24. URL: https://spravochnick.ru/filosofiya/problema_smerti_i_bessmertiya_lichnosti/ (дата обращения: 29.03.2021).
3. Проблема бессмертия человека: философско-антропологический и религиоведческий аспекты [Электронный ресурс] // CYBERLENINKA. URL: https://cyberleninka.ru/article/n/problema-bessmertiya-cheloveka-filosofsko-antropologicheskiy-i-religiovedcheskiy-aspekty (дата обращения: 29.03.2021).

Секция 1.4

О ЗАЩИТЕ ИНФОРМАЦИИ В ГОДЫ ВОЙНЫ

Бузов Кирилл Игоревич, студент 1-го курса
Научный руководитель Сергеев Александр Васильевич, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС»,
г. Старый Оскол

Вспоминая о Второй мировой войне, принято говорить о подвигах людей, сражавшихся на фронте или обеспечивавших армию в тылу. При этом почему-то забывается другая важная составляющая войны – информационная. Не провизия, не боевое снаряжение и даже не люди порой решали исход сражения. Главным ресурсом на поле битвы всегда являлась информация.

Информация поступает в каждую часть земного шара, связывая ее с остальным миром и поддерживая в ней жизнь. В военное время ее значение еще большее увеличивается: от того, какие данные содержатся в сообщении, могут зависеть сотни тысяч жизней. В таких условиях необходимость обеспечения безопасности информации является приоритетной задачей.

Наукой, которая определяет главные инструменты защиты информации, является криптография. За многовековую историю использования информации человечеством изобретено множество способов ее защиты, в том числе криптографических через шифрование данных.

После Первой мировой войны работы в этой области особенно оживились.Многие люди стали проявлять интерес к шифрованию, делая занятия криптографией своим хобби.Благодаря такой активности вместе с развитием и усовершенствованием шифров стали появляться различные технические устройства.

Самым известным из таких изобретений является знаменитая шифровальная машина «Энигма» (по-гречески – загадка). Она была изобретена в Голландии еще в 1919 году и предназначалась для гражданских целей, но позже патент на нее выкупили немцы и в 1926 году оснастили такими машинами три свои армии.

Машины «Энигма» использовали оригинальный способ кодирования и выпускались в нескольких вариантах. Создатели «Загадки» утверждали, что расшифровать ее сообщения вручную невозможно в принципе.

Однако работа по расшифровке кодов «Загадки» велась постоянно, и облегчили ее противникам сами немцы. Расшифровку упростил стандартный язык сообщений, где выражения и слова часто повторялись, и сотрудники с родным немецким языком могли их отследить. В сообщениях подводникам слово «погода» было обязательным, а немецкая грамматика ставила его на точное место в предложении. Еще немцы часто употребляли слова «фатерланд» («отечество») и «рейх» («государство»). Кроме того, дешифровку облегчала лень некоторых радистов, которые по 2-3 дня не меняли настройки.

Начиная с 1939 года сначала поляки, а вслед за ними французы и англичане могли расшифровывать сообщения «Энигмы» и в течение всей войны знали планы Германии.

Например, 1 и 8 августа 1940 года были перехвачены приказы штаба Геринга о подготовке к массовой бомбежке военно-воздушных баз Англии, а 12 августа – приказ о первом таком налете. Командование королевских ВВС сумело принять необходимые меры.

В дальнейшем англичане и их европейские союзники регулярно получали сведения о предстоящих атаках, но то, как эта информация была получена, они старались держать в

строжайшей тайне.Для конспирации пришлось даже пожертвовать целым городом: было перехвачено сообщение о предстоящем налете на город Ковентри, но для его обороны ничего не было принято, и город был полностью разрушен.

Решение задачи взломанемецких шифров привело к новой проблеме: приходилось быстро проводить огромное количество вычислений. Для этих нужд в Великобритании в 1943 году под руководством Алана Тьюринга была построена мощная электроннаясчетно-вычислительная машина «Колосс», которая сокращаласрок расшифровки шифров «Энигмы» до 24 часов. Британское правительство на протяжении 30 лет рассматривало ее проект как военную тайну, поэтому она не стала базой для дальнейшего развития компьютеров. Но это был первый в мире электронный компьютер.

Немцы постоянно совершенствовали «Энигму». Операторов натаскивали на ее уничтожение в случае опасности. Ключи во время войны меняли каждые 8 часов. Шифродокументы растворялись в воде. Однако до конца войны немцы так и не узнали, что секрет их «Загадки» известен противникам.

Союзническими обязательствами предусматривался обмен полученной от противника информацией. Например, в июне 1943 года Черчилль сообщил Сталину о предстоящем наступлении германских войск в районе Орла, Курска и Белгорода. Известно еще о нескольких таких предупреждениях, но почти все они были сделаны слишком поздно.

Советская разведка не дожидалась проявления доброй воли со стороны союзников и в течение всей войны стремилась своими силами добывать стратегическую информацию.

В 1937 году в Ленинграде был образован комбинат техники особой секретности, на котором уже в 1939 году была выпущена первая советская шифровальная машина М-100 «Спектр», а в серийное производство запущенна машина Ка-37 «Кристалл».

На машинную шифросвязь в годы войны легли огромные нагрузки. Только шифровальной службой Генштаба сухопутных сил было отработано 1,5 миллиона шифротелеграмм.

В полевых условиях часто использовалось и ручное шифрование. Войсковым шифровальщикам доводилось работать в исключительно сложных условиях. По инструкции Генерального штаба они обеспечивались усиленной охраной, но случалось и так, что вместо охраны шифровальщик ставил перед собой канистру с бензином, укладывал рядом гранаты и вынимал из кобуры пистолет. Ценность собственной жизни отступала на второй план, главное – передаваемые данные и шифровальная техника.

В боевых условиях телеграммы часто отправлялись с помощью радиостанций «Север», которые также выпускалась в блокадном Ленинграде. Военные связисты ласково называли ее «Северок».Немецкое командование обещало высокую награду за захват «Северка» с радистом, но это не удалось ни одному карательному отряду.

Благодаря развитию специализированной техники и криптографических методов накануне Великой Отечественной войны советские дешифровальщики предупредили руководство страны о предстоящем нападении Германии, а в ходе войны предоставили руководству страны огромное количество важнейшей информации.

Героический и напряжённый труд военных криптографов в период войны был высоко отмечен командованием.

Достойно оценилиработу советских шифровальщиков полководцы Жукови Василевский.

Оценил работу советской шифрослужбы и противник. По распоряжению Гитлера: «… кто возьмет в плен русского шифровальщика либо захватит русскую шифровальную машину, будет награжден Железным крестом, отпуском на родину и будет обеспечен работой в Берлине, а после победы – поместьем в Крыму».

Уроки войны заставили правительство Советского Союза по достоинству оценить значимость уровня криптозащиты государства и в корне пересмотреть свое отношение к шифрослужбам. К концу 40-х годов XX века было создано Главное управление специальной

связи, к государственной криптографической работе были привлечены математики высокого класса, а в МГУ им. Ломоносова стали готовить математиков-криптографов.

Список использованных источников

1. Защита информации во время Великой Отечественной Войны [Электронный ресурс].-URL:https://www.pvsm.ru/news/7164(дата обращения: 18.03.2021).
2. Информационная безопасность времен Второй мировой: взлом «Энигмы» [Электронный ресурс]. - URL: https://www.kaspersky.ru/blog/ww2-enigma-hack/7715/(дата обращения: 18.03.2021).
3. Шифровальная служба Советского Союза [Электронный ресурс]. - URL: https://topwar.ru/152518-shifrovalnaja-sluzhba-sovetskogo-sojuza-okonchanie.html (дата обращения: 16.03.2021).

ИССЛЕДОВАНИЕ ВЛИЯНИЙ АВТОКОЛЕБАНИЙ НА ПРОЦЕСС РЕЗАНИЯ

Качановский Александр Русланович, студент 4-го курса
Научный руководитель Ушакова Юлия Альбертовна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Возникновение вибраций при обработке резанием характеризуется возмущающими силами и свойствами упругой системы. Колебания (вибрации) при резании бывают, как правило, двух типов: вынужденные, когда причиной колебаний является периодически действующая возмущающая сила, и автоколебания.

Способы борьбы с вынужденными вибрациями хорошо известны - необходимо устранить действие периодической возмущающей силы. Это достигается балансировкой инструмента (шлифовальных кругов, фрез, резьбовых головок) и заготовок, виброизоляцией фундаментов станков и т.д.

Значительно более сложной задачей является гашение вибраций, имеющих автоколебательный характер. Автоколебания при резании относятся к классу самовозбуждающихся вибраций, присутствие которых при обработке металла оказывает негативное влияние на качество поверхности и размерную точность обрабатываемой детали. Также это негативно отражается на стойкости резца и даже на долговечность станка.

Причины возникновения автоколебаний при резании следующие: уменьшение сил трения при увеличении скорости резания, образование и срыв нароста, периодический процесс упрочнения материала, запаздывание сил резания при перемещениях инструмента и пр.

Например, изменение припуска вызывает изменение силы резания, которая провоцирует изменение упругой деформации всей технологической системы что, в свою очередь, вызывает соответствующее изменение глубины резания. Таким образом, автоколебания возникают и поддерживаются за счёт внутренних процессов замкнутой технологической системы, которая имеет внешний источник энергии.

Управлением уровнем автоколебаний можно достичь повышения производительности обработки за счёт интенсификации режима резания. Геометрические параметры обработанной поверхности также существенно зависят от уровня амплитуды автоколебаний и их частоты. Поскольку динамика станков объясняет возникновение автоколебаний многими причинами, в том числе и наличием сложных многокоординатных связей в упругой системе, то для построения адекватной математической модели нельзя ограничиться всего одной координатой. Для теоретического исследования условий устойчивости и возникновения автоколебаний необходимо, как минимум, рассмотреть технологическую систему ТОС, представленную в виде взаимосвязанной двухкоординатной динамической модели. Кроме того, поскольку одной из основных причин возникновения автоколебаний всеми исследователями отмечается обработка «по следу», то такое важное возмущение также должно быть учтено в математической модели ТОС, которая должна отображать замкнутость всей системы через процесс резания. Исходя из таких соображений, для построения математической модели ТОС можно воспользоваться динамической моделью поперечного сечения токарного станка.

Цель исследования заключается в исследовании и анализе влияния параметров резания при токарной обработке на устойчивость процесса обработки, а также влияние этих параметров на возникновение автоколебаний в технологической системе при резании [2].

В данной работе практическая часть исследования автоколебаний при резании осуществляется с помощью прикладной программы, предоставленной кафедрой технологии

и оборудования в металлургии и машиностроении им. В.Б.Крахта СТИ НИТУ «МИСиС». Эта программа моделирует реальные физические процессы обработки резанием и построена на базе математической модели, которая адекватно отражает известные из практики характеристики процессов резания.

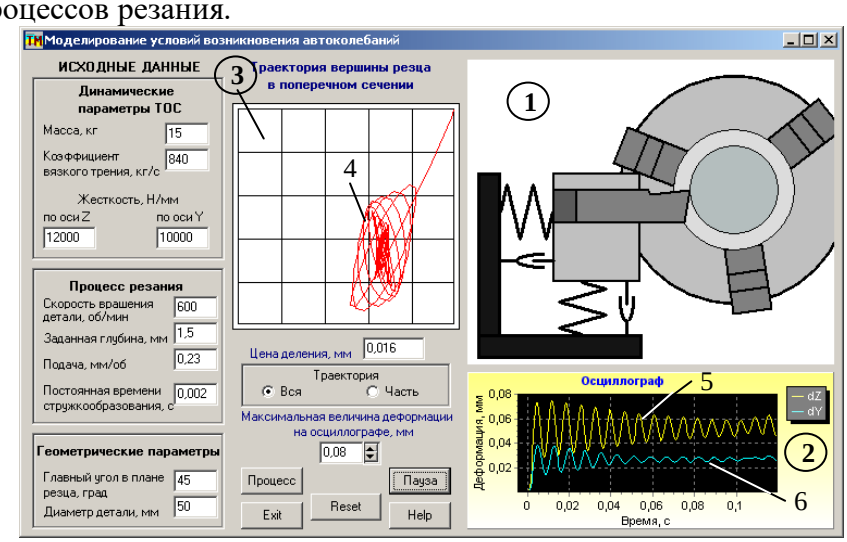


Рисунок 1- Математическая модель

В окне математической модели (см. рис.1) отображается траектория движения вершины резца по координатам *Z* и *Y*, то есть в вертикальном сечении заготовки. На изображении осциллографа (окно 2) появляются осциллограммы характеристик резца: линия *5* — деформация по координате *Z*, линия *6* — деформация по координате *Y*.

В зависимости от динамических характеристик ТОС дальше наступают или установившиеся колебания, которые определяют уровень вибраций в системе во время обработки, или амплитуда колебаний постоянно увеличивается, что будет определять потерю устойчивости и так называемое подрывание. В таком случае, реально, процесс резания продлеваться не может. Для определения приведённых тенденций необходимо оценивать процесс не менее чем через 5 оборотов заготовки.

Первая серия экспериментов в проводилась для определения зависимостей амплитуды колебаний технологической системы и приведённой массы динамической системы. Принятый шаг изменения массы 5 кг. Данные первого эксперимента приведены в таблице 1.

Таблица 1 - Зависимость амплитуды колебаний от C_z для m = 15кг

№ эксперимента	C_z, Н/мм	m = 15 кг = const	
		δ_z, мкм	δ_y, мкм
1	11000	н. у.	н. у.*
2	11500	9	2
3	12000	21	3
4	12500	13	2
5	13000	2	0
6	13500	2	0
7	14000	4	1
8	14500	2	0
9	15000	2	0

*- неустановившийся процесс резания.

По результатам проведённых экспериментов, с использованием пакета Excel построены графики соответствующих зависимостей (см. рис. 2).

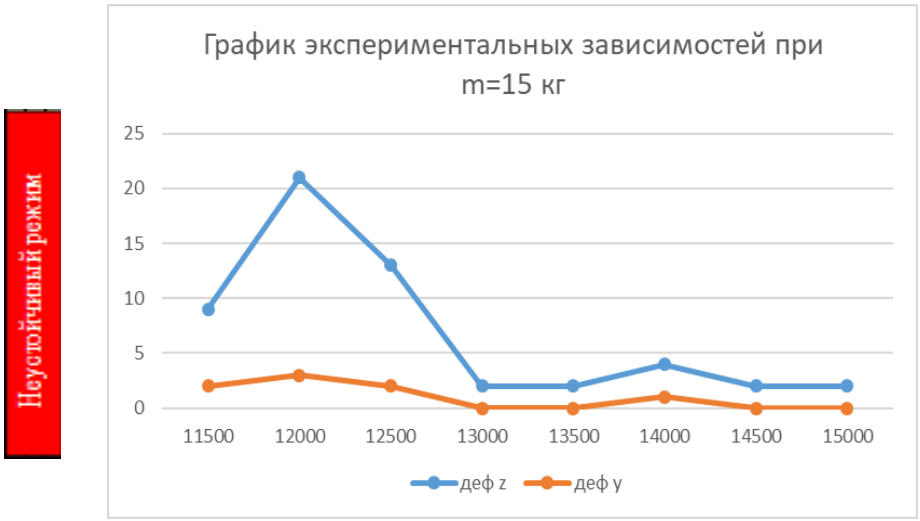


Рисунок 2 - Графики экспериментальных зависимостей амплитуды колебаний при m = 15 кг

Вторая серия экспериментов в проводилась для определения зависимостей амплитуды колебаний технологической системы и частоты вращения заготовки. Данные первого эксперимента приведены в таблице 2.

Таблица 2 - Зависимость амплитуды колебаний от частоты вращения заготовки

№ эксперимента	$n_з$, об/мин	$t_{5об}$, с	V, м/мин	δ_z, мкм	δ_y, мкм
1	450	0,67	71	н. у.	н. у.
2	550	0,55	79	18	4
3	650	0,46	102	20	5
4	750	0,40	118	12	1
5	850	0,35	134	7	2
6	950	0,32	149	10	3
7	1050	0,29	165	11	3
8	1150	0,26	181	2	0
9	1250	0,24	196	4	0
10	1350	0,22	212	6	1
11	1450	0,21	228	3	0
12	1550	0,19	243	4	0

По результатам проведённых экспериментов, с использованием пакета Excel построены графики соответствующих зависимостей (см. рис. 3).

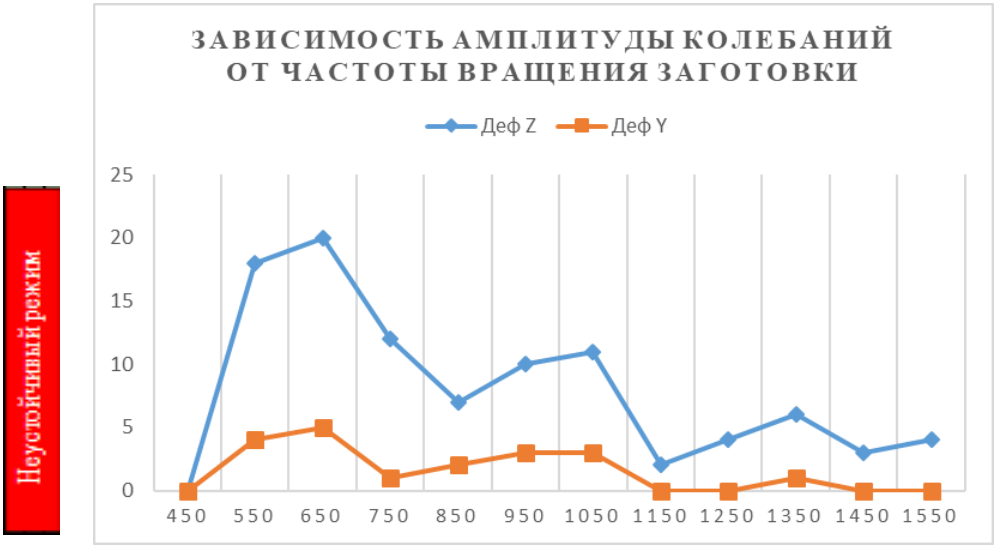


Рисунок 3- Графики зависимостей амплитуд автоколебаний по осям Z и Y от частоты вращения заготовки

Из первого эксперимента можно сделать вывод, что режим работы ТОС при резании существенно зависит от жёсткости Cz по координате Z. Зависимость имеет периодический характер и определяет такие режимы работы: при Cz<11000 Н/мм — неустойчивый режим, при 11000 Н/мм<Cz<15000 Н/мм — режим установившихся автоколебаний, при Cz>15000 Н/мм — устойчивый режим работы без автоколебаний. Неустойчивый режим при жёсткости Cz< 11000 Н/мм характеризуется постепенным увеличением колебаний, однако, на практике, при таком режиме после существенного увеличения сечения срезаемого слоя, происходит поломка или инструмента, или детали. Приведённая масса упругой ТОС также существенно влияет на динамическую частотную характеристику системы, а именно, на сдвиг границы устойчивости по жёсткости Cz. При увеличении массы с 10 кг до 20 кг граница устойчивости по жёсткости сдвигается с 9000 Н/мм до 12000 Н/мм.

Из второго эксперимента можно сделать вывод, что амплитуда колебаний является частотной характеристикой упругой ТОС, замкнутой через процесс резания. В этом случае наблюдается существенное влияние частоты вращения заготовки на режим работы. В ходе экспериментов была выявлена зона неустановившегося режима резания при $n_з$<450 об/мин, и зона установившихся автоколебаний. Здесь, кроме влияния частотных факторов, ощущается также влияние уменьшения силы резания при увеличении скорости от 60 м/мин до 200 м/мин. По результатам проведённых экспериментов для реальных процессов можно рекомендовать повышение частоты вращения заготовки и увеличение скорости резания; увеличения массы ТОС; балансировка быстро вращающихся элементов станка.

Список использованных источников

1. Петраков Ю.В., Драчев О.И. Моделирование процессов резания: учебное пособие. - 2-е изд., перераб.- Старый Оскол: ТНТ, 2018 - 240 с.
2. Петраков Ю.В., Драчев О.И. Автоматическое управление процессами резания: учебное пособие. - Старый Оскол: ТНТ, 2018 - 408 с.

АНАЛИЗ ВЛИЯНИЯ СКОРОСТИ РАЗЛИВКИ НА ОКАЛИНООБРАЗОВАНИЕ

Коротких Иван Игоревич, студент 4 курса
Научный руководитель Гришина Светлана Сергеевна,
преподаватель высшей, категории

Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,

г. Старый Оскол

АО “ОЭМК” является современным металлургическим предприятием, на котором в настоящее время освоено производство около 2000 марок качественных углеродистых и легированных сталей.

Разливка стали осуществляется на машине непрерывного литья заготовок (МНЛЗ). Непрерывная разливка стали на МНЛЗ состоит в том, что жидкий металл непосредственно из ковша или через промежуточное устройство непрерывно заливается в верхнюю часть водоохлаждаемого кристаллизатора, в который предварительно вводят затравку того же поперечного сечения, что и слиток. Верхний торец затравки служит дном для первых порций металла. По мере затвердевания отливаемая заготовка с помощью тянущих механизмов вытягивается вниз, формируя непрерывно литую заготовку (рис.1). Толщина затвердевшей корочки на выходе из кристаллизатора должна быть в пределе от 25 до 30 мм, чтобы обеспечить достаточную механическую прочность вытягиваемой заготовки и исключить возможность прорыва жидкого металла.

Рисунок 1 – Непрерывно литая заготовка

Температура поверхности слитка на выходе из кристаллизатора колеблется от 1100 до 1200°С при средней температуре корочки 1300 – 1350 °С. Слиток с затвердевшей корочкой, попадающий из кристаллизатора в зону вторичного охлаждения, в результате форсированного поверхностного охлаждения затвердевает по всему сечению. Форма слитка сохраняется за счет специальной поддерживающей системы. После прекращения подачи воды слиток охлаждается на воздухе[1].

В конце зоны вторичного охлаждения температура поверхности (tп) слитка снижается до уровня 800-900°С. Слиток принудительно вытягивается с помощью тянущих клетей, а затем поступает в газорезку, где разрезается на мерные куски заданной длины. Далее заготовки по рольгангу транспортируются на склад.

Одна из проблем при разливке стали – образование окалины. В металлургическом процессе от разливки до проката образуется достаточно много окалины, что не посредственно приводит к потере годного металла и следственно финансовые потери производства.

Так, разберём, что такое окалина. Окалина — это смесь оксидов, образующихся прямым действием кислорода при накаливании на воздухе металлов. Окалинообразование - процесс появления на поверхности металла слоя высокотемпературного окисла, с заметной скоростью начинает происходить на наиболее распространенных марках конструкционных сталей при температуре от 700 ^{0}С и выше.

Толщина и масса окалины возрастает с увеличением температуры и длительности нагрева стали. Скорость окисления сталей, как и чистого железа, подчиняется параболическому закону при окислении на воздухе, в углекислом газе и водяном паре.

Рисунок 2 – Окалина на слитке стали

Проблема изучения процессов высокотемпературного окисления включает установление скорости роста окалины в зависимости от различных факторов, главным образом температуры, продолжительности окисления или скорости охлаждения, механизма роста окалины, ее структуры[2].

Целью исследования является проблема образования окалины.

Для выявления зависимости между скоростью разливки и количеством образования окалины в работе были проведены расчеты. В качестве исходных данных приняли: массу плавки - 170т, масса 1 метра непрерывно литой заготовки сечением 300х360 – 0,83т, скорость разливки от 0,45 до 0,7 м/мин. На основании практических данных установили, что при скорости разливки 0,45 м/мин образуется слой окалины 0,1 мм.

Результаты расчетов представлены в табл.1.

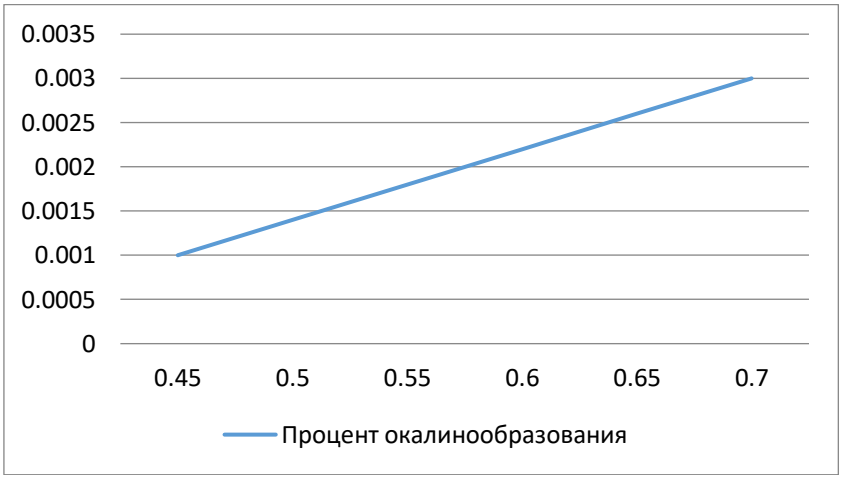
Таблица 1 – Количество окалины образующейся при выплавке стали массой 170т

Скорость разливки, м/мин	Толщина окалины, м	Масса окалины, кг/м заготовки	Масса окалины всей плавки, кг	Масса годной заготовки без учёта окалины, м/кг	Масса годного металла со всей плавки, кг	Доля окалины на всю плавку, %
0,45	0,001	5,94	1216,627	824,06	168783,4	0,720821
0,5	0,0014	8,316	1703,277	821,684	168296,7	1,012068
0,55	0,0018	10,692	2189,928	819,308	167810,1	1,305004
0,6	0,0022	13,068	2676,578	816,932	167323,4	1,599644
0,65	0,0026	15,444	3163,229	814,556	166836,8	1,896002
0,7	0,003	17,82	3649,88	812,18	166350,1	2,194095

Скорость окисления, а в конечном итоге, количество образующейся окалины и ее свойства, определяются диффузионными и кристаллохимическими процессами, происходящими внутри окалины, а также на ее границах с металлом и окисляющей средой.

Структура окалины зависит от множества факторов, связанных с химическим составом стали, условиями образования окалины, температурным режимом охлаждения готового изделия. Если окисление происходит на воздухе при температурах до 570° С, то в составе окалины могут находиться только два окисла: магнетит (Fe_3O_4) и гематит (Fe_2O_3). При температурах, превышающих 570 °С, все основные окислы железа устойчивы и в окалине может возникать еще и третья фаза — вюстит (FeO).

На основании этой таблицы был составлен график окалинообразования.



На основание полученных результатов, был сделан вывод, что процент окалины от всей массы плавки увеличивается прямо пропорционально увеличению скорости разливки на МНЛЗ.

Список использованных источников

1. Бигеев В.А., Основы металлургического производства: учебник / В.А. Бигеев, К.Н. Вдовин., В.М. Колокольцев – Санкт-Петербург: Издательство Лань-Трейд, 2017. - 616 с.
2. https://markmet.ru/kniga-po-metallurgii/umenshenie-okalinoobrazovaniya-pri-proizvodstve-prokataческих свойств отходов прокатного производства и трудности их утилизации.

ИЗГОТОВЛЕНИЕ МОДЕЛИ ГЕНЕРАТОРА ПЕРЕМЕННОГО ТОКА

Кузнецов Павел Владимирович, Камынин Сергей Алексеевич, студенты 1-го курса
Научный руководитель Амельчакова Елена Анатольевна,
преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Машина, превращающая механическую энергию в энергию переменного тока с использованием явления электромагнитной индукции, называется генератором переменного тока. Это приспособление было изобретено в 1832 году благодаря открытию Николы Тесла. Тогда был создал первый однофазный синхронный генератор переменного электрического тока. Первые установки производили только постоянный ток, а рассматриваемый генератор переменной характеристики находил своего практического применения. Но люди быстро поняли, что переменный ток использовать гораздо практичнее, чем постоянный.

В генераторе переменного тока магнитное поле создаётся электромагнитом, питаемым постоянным током. Допустимая сила тока ограничивается нагреванием скользящих контактов- щёток. В генераторах переменного тока большой магнит является ротором. При вращении ротора возникает переменная ЭДС индукции в обмотках, расположенных в неподвижной части-статоре. Чтобы увеличить ЭДС индукции, используется обмотка с большим числом витков. Для увеличения магнитного потока эту обмотку наматывают на стальной сердечник и зазор между сердечниками ротора и статора делают как можно меньше.

Генераторы переменного тока применяют уже достаточно давно. За последние годы сфера применения стала еще более обширной. Производственные электроустановки являются выгодным вариантом для генерации электроэнергии, используемой на заводах и предприятиях, учебных учреждениях, торговых центрах и т. д. Также такие генераторы позволяют значительно ускорить строительство сооружений в тех местах, где нет возможности провести линию электропередачи.В быту такие устройства такие устройства применяются для питания частных домов, дачных участков или коттеджей.

Нас заинтересовала модель электромагнитного генератора. Это приспособление состоит из неподвижного магнита и проволочной рамки. Её концы соединяются между собой при помощи контактного кольца, которое скользит по электропроводной угольной щетке.

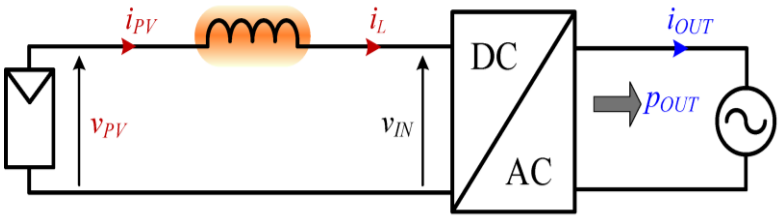
Электрический индуцированный ток переходит к внутреннему контактному кольцу в тот момент, когда половина рамки, соединяющаяся с ним, проходит мимо северного полюса магнита и, наоборот, к внешнему кольцу в тот момент, когда другая часть проходит мимо северного полюса. Экономичным способом, на котором основывается принцип работы генератора переменного тока, является сильная выработка. Этогоможно достичь использованием одного магнита, который вращается относительно нескольких обмоток. При помещении его в проволочную катушку, он начнет индуцировать электрический ток, что будет причиной отклонения стрелки гальванометра. Когда магнит будет вынут из кольца, ток поменяет свое направление, а стрелка прибора отклонится в другую сторону.

Для изготовления генератора мы изучили соответствующую литературу, выполнили чертёж, подобрали компоненты для сборки.

Модель электромагнитного генератора состоит из:

1. Катушек из медного провода с сердечником - 2-4 штук(примерно 50 витков).
2. Магнитов- 4 штук.
3. Диска из ДСПи квадратной основы.
4. Креплений.

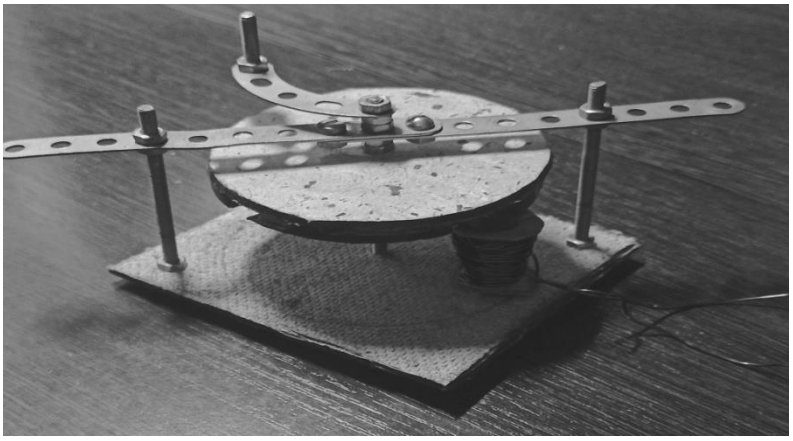
Генератор был собран по схеме:



При сборке возникли проблемы:

1. Поиск подходящей проводки, и намотка проводки на катушку.
2. Дефекты изоляционного слоя медного провода.

Полученная модель электромагнитного генератора представлена на фотографии.



В ходе работы над проектом мы познакомились с принципом работы генератора переменного тока, видами генераторов и их характеристиками, применением в быту и промышленности.

Список использованных источников

1. https://xteoretegx.livejournal.com/ LIVEJOURNAL [Электронный ресурс]
2. Studwood.ru [Электронный ресурс]:https://studwood.ru/ Studwood.ru [Электронный ресурс]

СОВЕТЫ ПО ЭКОНОМИИ ЭЛЕКТРИЧЕСТВА ДОМА

Легостаев Артем Сергеевич, Ильин Сергей Сергеевич, студенты 2-го курса
Научный руководитель Боровская Ираида Владимировна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
Оскольский политехнический колледж,
г. Старый Оскол

В настоящее время электричество играет важную роль в нашей жизни. Без него не обходится ни дом, ни фабрика, ни учреждение. Но в то же время электричество опасно. Например, если вы прикоснетесь к электрическому устройству мокрыми руками, то можете получить удар электрическим током. Поэтому необходимо соблюдать правила безопасности. Разумно используя электричество, мы улучшаем нашу жизнь. Большое количество научных открытий связано с электричеством. Бурное развитие науки об электричестве было получено, когда в 1800 году Александр Вольт изобрел первый надежный и постоянный источник энергии, принесший с собой все важнейшие открытия в этой области.

Трудно представить нашу жизнь без электричества. По пути подведены электрические сети, в квартире есть бытовая техника. Поэтому, если мы представим себе, что однажды электричество исчезнет по всей планете одновременно, человеческая жизнь резко изменится. Мы уже не можем быть без электрического тока, потому что он приводит в движение и приводит в действие почти все механизмы и устройства, изобретенные человеком. Электричество - это спутник и помощник одновременно.

Электроэнергетика, конечно, отличная компания, но нужно знать, как ею правильно управлять. В противном случае вы можете столкнуться с множеством ошибок и недочетов. Именно поэтому приглашаю всех подружиться с электричеством, ведь без него нам очень сложно жить.

Советы о том, как сэкономить деньги, должны стать чем-то вроде плана для каждого. Прогнозирование затрат, покупка только необходимого, поиск более выгодных альтернатив - все это может быть связано как с семейной экономикой, так и с предпринимательством.

Немного рекомендаций экономии электричества дома:

1) Проверьте, не стоит ли холодильник возле плиты или радиатора. Конечно, не все типы холодильников легко переставляются, но при желании нет ничего невозможного. Обратите внимание, что расстояние между стенкой холодильника и задней стенкой должно быть не менее 5-10 см. Избегайте попадания прямых солнечных лучей на корпус холодильника и никогда не кладите в него горячие продукты;

2) Оптимально используйте тепло утюга. Гладить лучше всего, когда накопилось много белья, не отвлекаясь на телевизор, не ходя в магазин и не разговаривая по телефону. Ведь железо потребляет много электричества, и было бы наивно тратить его зря;

3) Налейте в чайник ровно столько воды, сколько вам нужно на данный момент. Остерегайтесь известняка. Его наличие значительно увеличивает потребление энергии. Владельцам газовых плит лучше вообще не пользоваться электрическим чайником;

4) Если у вас дома есть электрическая плита, следите за тем, чтобы посуда не соприкасалась с конфорками. Вы можете потерять до 50% электроэнергии, если предположите, что сковорода не идеально подходит для сковороды. Также выбирайте сковородку правильной окружности для любого кухонного инвентаря. За 3-5 минут до готовности еды можно смело выключать плиту. Остального тепла хватит, чтобы блюдо вернулось в форму.

5) Вспомните, как в детстве на нас кричали родители - выключите свет за спиной! И они были правы. Отключение ненужного света - главное правило энергосбережения. Это

правило не так актуально, если у вас повсюду стоят энергосберегающие лампочки или датчики движения, которые автоматически выключают свет, когда вы выходите из здания.

6) Различные обогреватели окон и аккумуляторы хорошо экономят электроэнергию. Приобретайте электроприборы класса энергопотребления «А» и выше. Они будут стоить дороже, но в конечном итоге вы не только сэкономите, но и поможете природе. Самое главное - это ваша организация и ваше желание экономить энергию.

7) Применяйте датчики движения в собственном доме (автоматически выключайте и включайте свет в комнате, в которую входит человек)

8) Подключение и установка автоматического выключателя. (Выходя из дома, человек может выключить все электрические устройства, которые взаимодействуют в режиме ожидания, и оставить необходимые, например, холодильник)

9) Установка двух тарифного счетчика, который считает день и ночь. Ночью стоимость оплаты 1,11 руб., днем 1,72 руб. за 1 кВт

Электроэнергия поступает в наши дома от различных типов электростанций, а для ее производства сжигаются уголь, нефть и газ. Экономное использование электроэнергии позволяет снизить потребление энергоресурсов и, как следствие, снизить выбросы вредных веществ в атмосферу, сохранить чистоту водоемов. Экономя энергоресурсы, каждый из нас может внести свой вклад в общее дело сохранения природы.

По статистике, средняя российская семья тратит около 10% своего дохода на оплату жилищно-коммунальных услуг. Большая часть этих затрат приходится на оплату электроэнергии. Таким образом, экономя электроэнергию, вы можете значительно сократить расходы на оплату счетов. Ведь стоимость электроэнергии напрямую связана со стоимостью топлива, запасы которого ограничены, а цены постоянно растут.

Конечно, в современном мире вообще невозможно обойтись без освещения и бытовых электроприборов. Однако есть простые способы снизить ежедневное потребление энергии, доступные каждому.

Лучшее из них - это экономия света. Для этого не нужно сидеть в темноте. Полностью замените обычные лампы накаливания компактными люминесцентными лампами (КЛЛ), потребляющими гораздо меньше энергии. На первый взгляд их цена (150-200 рублей за лампу) очень удивляет, но даже при такой высокой стоимости они быстро окупаются за счет небольшого энергопотребления и длительного срока службы.

Например, наша семья платила в среднем 302,72 рубля в месяц. Однако мы подсчитали, что потратим 213,28 рубля в месяц, если отключим от сети все электроприборы, когда они не потребляются. Но если бы при этом наблюдали отключение ненужных ламп, наша стоимость составила бы 172 рубля. Заменив некоторые лампы накаливания на энергосберегающие, наша семья уже почти в 2,5 раза экономит.

Моей семье показалось довольно интересным сделать вывод, что отключение электроприборов от розетки - это неплохая экономия.

Список использованных источников

1. Данилов, Н.И. Энергосбережение - от слов к делу / Н.И.Данилов.- Екатеринбург, Энерго-Пресс, 2000.
2. Епишков, Н.Е. Энергосбережение - базовая технология создания эффективного сельского хозяйства

ЭКОНОМИЧЕСКОЕ ОБОСНОВАНИЕ РАЗРАБОТКИ И МОДЕЛИРОВАНИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ КОЗЛОВОГО КРАНА

Львов Леонид Владимирович, Сорокин Никита Олегович, студенты 4-го курса
Научный руководитель Некрасова Елена Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Любая автоматизация производства предполагает выполнение всех стадий технологического процесса согласно предварительно заданной программе и без непосредственного участия человека.

Автоматизация бывает частичной либо комплексной. Проводится она в соответствии с принятым планом модернизации производства. Любое промышленное предприятие предполагает использование крупногабаритных грузоподъемных кранов.

Для автоматизации управления такими машинами, необходимо сосредоточить внимание на отдельных операциях:

- запуске, торможении механизмов;
- подборе оптимальной скорости рабочих движений;
- фиксации частей крана в нужном положении и так далее.

Для решения подобных задач созданы командоконтроллеры и автоматизированные устройства безопасности - ограничители крайних положений и грузоподъемности, грузозахваты, противоугонные средства. Даже частично автоматизированный кран отличается повышенной производительностью. Такая машина быстрее выполняет работу и требует меньшего количества обслуживающего персонала при перемещении груза.

На рисунке 1 представлен общий вид козлового крана.

Необходимость автоматизации управления кранами возникает в том случае, если ввиду напряженности производственного цикла человек попросту не успевает контролировать их работу.

Полная автоматизация актуальна для предприятий, выпускающих изделия серийно и массово. В таком случае всеми операциями управляет компьютер. Для отдельных видов грузоподъемного оборудования (грейферных кранов, подвесных конвейеров, штабелеров) задействуют электромеханические выключатели.

Применения системы дистанционного управления, позволит увеличить скорость проведения работ, уменьшить временные потери, обеспечить высокую точность операций с грузом на удаленном расстоянии.

Удобство и безопасность. Повышение производительности. Сокращение численности обслуживающего персонала. Одновременное управление несколькими кранами с одного пульта дистанционного управления краном.

Рисунок 1 - Общий вид козлового крана

Козловые краны выполняют функции перегрузки, строительства, ремонта и монтажа во всех отраслях промышленности, обслуживая машиностроительные заводы, ж/д станции, кирпичные, металлургические, лесозаготовительные предприятия, атомные и гидроэлектростанции. Такая востребованность автоматизированных козловых кранов на производственных и стратегически важных объектах обуславливается экономической целесообразностью. Стоимость козловых кранов, за счет отсутствия необходимости возведения крановых эстакад, составляет на 40–60% меньше стоимости мостовых кранов.

Модель состоит из рельс передвижения, опорных рам, балки для каретки с кареткой и блока управления приводами передвижения благодаря которым осуществляется манипуляции с грузами по их перемещению.

Управляет всем этим микроконтроллер ATmega328P.

Для создания автоматизированной системы козлового крана необходимы следующие элементы:

- Микроконтроллер – ATmega328P, стоимость которого составляет - 1600 руб.;
- Редукторные двигатели постоянного тока Transtecno общая стоимость которых - 2400 руб.;
- Беспроводной Bluetooth приемопередатчик модуль RS232, стоимость которого - 126 руб.;
- Импульсный блок питания, стоимостью – 1500 руб.

Итого стоимость системы управления козловым краном составляет:

1600+2400+126+1500=5626 руб.

Таким образом, сумма произведенных капиталовложений в разработку автоматизированной системы козлового крана составила 5626 руб.

Затраты на монтаж и ввод в эксплуатацию системы составляют 7450 руб. и влючают в себя металлический каркас стоимость которого составляет 5250 руб., детали корпуса стоимостью 1900 руб.. Также использовался кабель сечением 3 мм^2, стоимость которого составляет 300 руб.

Автоматизация производственного процесса имеет очень важное практическое значение. Ведет ускорению производственного цикла и увеличению производительности.

Список использованных источников

1. Беспроводной Bluetooth приемопередатчик модуль RS232 [Электронный ресурс]: https://www.adafruit.com/product/rs232
2. Официальный Интернет-магазин Arduino [Электронный ресурс]: https://store.arduino.cc
3. Российское Ардуино-сообщество [Электронный ресурс]: https://arduinomaster.ru/
4. Сайт с общей информацией о промышленных козловых кранах [Электронный ресурс]: http://zpk-prom.ru/page/3?s&submit

ОБЩЕНИЕ КАК ЦЕННОСТЬ ЧЕЛОВЕЧЕСКОГО ОБЩЕСТВА

Мазницына Екатерина Вячеславовна, студентка 3-го курса
Научный руководитель Демба Ирина Михайловна,
преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Парадокс нашего времени

«Наши дома всё больше, а семьи всё меньше;
мы имеем больше удобств, но меньше времени.
Мы более образованы, но менее чувствительны;
у нас больше знаний, но меньше здравого смысла;
больше специалистов, но еще больше проблем;
больше лекарств, но меньше здоровья.
Мы проделали долгий путь до луны и обратно, но нам сложно перейти улицу, чтобы познакомиться с новым соседом.
Мы создали множество компьютеров для хранения и копирования большего количества информации, но нам не хватает общения.
Мы выиграли в количестве, но проиграли в качестве.
Это время быстрого поглощения, но медленного усвоения,
Людей высокого роста, но низкой нравственности,
высоких доходов, но мелочных отношений.
Это время, когда так много за окном, но ничего в комнате».

Его Святейшество Далай-лама XIV

Кризис общения в современном мире

Современное общество переживает многие кризисы: финансовый демографический, управленческий,кризис квалифицированных кадров и так далее. За все этим многообразием становится совсем незаметен кризис общения, который всё больше распространяется по человеческому обществу,охватывая все его возрасты и классы вот уже второе десятилетие.

Размышляя над высказыванием Далай-ламы, понимаем, что он говорит о кризисе духовности, и это, как никогда, актуально для современного времени. Низкий уровень индивидуального развития личности, мелочные отношения между людьми, нехватка человеческого общения, а зачастую и просто неумение общаться свидетельствуют об этом.

В течении последних 20 лет в нашем обществе произошло больше изменений, чем за всю предшествующую историю человечества. Эти изменения включают в себя огромные технологические усовершенствования, которые сделали общение более быстрым, более эффективным и энергичным.

Технологические перемены, несомненно, ведут к ускорению и интенсификации общения. У нас теперь есть электронная почта, многофункциональные телефоны, социальные сети, но стали ли мы эффективнее общаться? Нет.

Однако человек по природе - существо социальное. И воспитывались мы чаще в традиционной манере - общаясь с родителями, педагогами и сверстниками. Поэтому и испытываем от такой подмены реального общения виртуальным некоторое неудобство, нехватку, недостаточность. Недостаток общения сильно бьет по психике. Отсюда и появляются всевозможные психические недомогания общества и отдельных его индивидов, так распространившиеся в последнее время.

У современных детей меньше возможностей общаться и обучаться социальным навыкам, чем это было прежде. Во многих домах семья крайне редко собирается за общим столом, чтобы пообедать или поужинать вместе. Родители, чаще всего заняты построением карьеры, зарабатыванием материальных благ, а дети предоставлены сами себе. Общие семейные дела могут стать качественным временем, когда прекрасно могут быть разрешены многие проблемы, преодолены тревоги и беспокойства, обиды и взаимонепонимание. Но поскольку такие встречи случаются крайне редко, отношения внутри семьи постепенно разрушаются.

Когда разрушается общение - падают бомбы и рвутся снаряды, будь то в семейном окружении, на рабочем месте или в глобальной политике. Профессор Стивен Хокинг из Кембриджа заметил, что «мировые проблемы могли бы быть решены, если бы мы сохранили способность разговаривать друг с другом». И эта мысль применима к любой ситуации.

Идёт речь о двух людях в рамках маленькой организации или о двух радикальных группировках в международном конфликте, если они не сумеют выстроить общение между собой, они никогда не смогут преодолеть разногласия. [1, с.15]

Значимость общения в человеческом обществе

Тревогу вызывает неумение нашего подрастающего поколения общаться с окружающими, их эгоистичность, замкнутость, неумение находить друзей, самим быть верными товарищами, эмоциональная глухота, равнодушие к самым близким. С годами эти качества не исчезают, а закрепляются, становятся устойчивыми свойствами личности. Таким человек нередко приходит в коллектив, не трудно предугадать,как сложатся его отношения с людьми [3, с.54].

Неуставные отношения в армии, моральное и физическое насилие молодых людей по отношению друг к другу, могут служить ярким примером таких отношений. Потому, мы должны учиться общаться сами и учить этому наших детей, помочь им приобрести познания о том, как складывается общение, при каких обстоятельствах оно бывает успешным, почему существует непонимание?

Проблема общения в психологии

Петровский А.В. так говорит о ценности и необходимости учиться общению. «Вы можете приобрести какие угодно большие знания, но пока вы не научитесь общаться с окружающими,все они будут совершенно бесполезны».

Понятие общение, как и любое понятие социальной психологии, прорабатывалось многими исследователями и имеет разнообразные трактовки. Общение привлекало также внимание социологов, педагогов и философов. Наиболее объемно это понятие представила Л.П.Буева, которая интерпретирует общение как процесс взаимосвязи и взаимодействия общественных субъектов (личности, групп), характеризующийся обменом деятельности, информации, опытом, способностями, умениями и навыками, а также результатами деятельности; как одно из необходимых и всеобщих условий формирования и развития общества и личности.

Сущность общения можно охарактеризовать следующими ключевыми словами: контакт, связь, взаимодействие, обмен, способ объединения. Наиболее точным словом для обозначения общения как социально - психологического феномена является слово контакт, т.е. соприкосновение. Контакт между людьми осуществляется посредством языка и речи. Речь является основным средством общения. Манера речи определяем мироощущение человека, его культуру. Содержание связано с информацией, отношение - с эмоциональным контекстом, который привносит в речь сам человек; воздействие определяется влиянием речи на другого или других [4, с. 120 -122].

Психологи давно установили, что замкнутые люди, которые не имеют друзей и мало общаются, становятся асоциальными. Это грозит возникновением психологических проблем. Одни зацикливаются на себе и своих состояниях. Так появляется ипохондрия. Сегодня эта

проблема очень распространена. Другие люди не делятся переживаниями, держат всё в себе. Они испытывают тяжесть ноши одиночества и становятся грубыми, черствыми.

Именно общение делает людей людьми. Это важнейший механизм, он заложен в человеке природой. И люди не должны забывать об этом. Да, без общения можно. Но это нанесёт, со временем, свой отпечаток на психику. Тогда как в общении человек исцеляется.

Философский взгляд на проблему общения

«Общение как вид человеческой деятельности очень сложный и многогранный процесс. Общение является объективной потребность каждого человека. Более того известный немецкий философ Людвиг Фейербах говорил по этому поводу следующее: «Человек всегда включен в систему общения с другими людьми, только в общении человек развивается в физическом и духовном смысле» [2, с. 68].

Не только философы 19 века так высоко оценивали роль человеческого общения в обществе. Современные философы также считают мир общения одной из фундаментальных категорий социальной философии. Проблемы общения становятся все более актуальными в связи с возрастающим дефицитом общения в современном мире, с обилием информации и электронных средств массовой коммуникации. Феномен общения сейчас привлекает все больше внимания своей комплексной основой, своей природой.

Л.А. Ситниченко пишет: «Обращение современной философии к проблеме общения как к одной из самых важных и самых «больных» связано с тем реальным обстоятельством, что общение не только опосредует познание человека и его деятельность, но и является условием самосознания личности и её развития». [5, с.93]. Таким образом, значимость проблемы заключается в том, что в общении человек развивается гармонично, а в не его одиночестве, отчуждённости людей друг от друга он становится чужд миру, прежде всего миру человеческому. Разрушить одиночество, тоску, страх и преодолеть эгоцентризм человека в урбанизированном обществе научно-технического прогресса можно, прежде всего, теплотой межличностных отношений, возвратом к первооснове социума - к живому межличностному общению.

P.S.: Проблема общения традиционно находится в центре внимания психологии и философии в связи с её значимостью во всех сферах жизнедеятельности человека и социальных групп. Ибо человек без общения не может жить среди людей, развиваться и творить.

Список использованных источников

1. Айви А.Е. Лицом к лицу. - Новосибирск, 2015.
2. Ильин В.В., Кармин А.С.,Философия. Учебное пособие. - Санкт-Петерберг, 2014.
3. Мещерякова Н.Я. Общение в подростковой среде. - М., 2004.
4. Петровский А.В. Учимся общаться. - М., 2010.
5. Ситниченко Л.А. Человеческое общение в современной западной философии. - М., 2005.

КОСМОС – ПОСЛЕДНИЙ РУБЕЖ

Майкова Ксения Федоровна, студентка 1-го курса
Научный руководитель Киреева Людмила Владимировна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС»,
г. Старый Оскол

Человеку во все времена был интересен космос. Но в силу технических возможностей мечты так и оставались мечтами, пока в 1950-х не началась космическая гонка между СССР и США. Итак, 4 октября 1957г., был выведен на орбиту первый искусственный спутник Земли. В дальнейшем СССР во многом стал первым: первые животные на орбите, полет Юрия Гагарина, выход человека в открытый космос – Алексей Леонов, но, несмотря на это США первые высадились на поверхность Луны. И тогда в новостях была произнесена знаменитая фраза «Это маленький шаг для человека, но огромный скачек для всего человечества»[4].

СССР не отставал, так в 1964 году началась программа по освоению Марса, но действительно стоящих результатов достиг «Марс-3». Он совершил мягкую посадку и передал первые в истории снимки Марса. Другая же программа под названием «Венера 7» совершила первую посадку на Венеру, так же было установлено, что у этой планеты невероятно высокое давление и она не близнец Земли.

Через несколько лет в 1975г. НАСА отправляют к Марсу два аппарата «Викинг 1» и «Викинг 2» для поиска следов жизни. Жизнь увы не нашли, но получили образцы грунта и первые цветные и панорамные снимки поверхности Марса.

Уже через 11лет СССР выводит на орбиту Земли постоянную станцию «Мир», на которой проведены сотни научных экспериментов.
В дальнейшем усилия всего человечества сложились в одно благое дело и в 1998г. станция стала Международной Космической. В этом проекте участвуют 14 стран. Одна из главных целей при создании станции – это возможность проведения различных опытов и экспериментов, которые требуют наличия уникальных условий космоса. В дальнейшем Космос приобрёл некоторый коммерческий облик.

Давайте посмотрим на количество полетов в космос разных стран. Мы видим, что начиная с 1960-х и до1990-хг. абсолютное лидерство удерживает СССР, но что потом? Начиная с 1992г. и заканчивая 2020г. Россия слетала в космос всего лишь 3 раза, но вот уже США начали более активную деятельность в этой сфере.

Для перспективного освоения лучше всего взять Марс. Основной проблемой является траектория полета. Из-за разной скорости движения планет и формы орбит, расстояние между Землей и Марсом меняется. Минимальное расстояние между планетами возможно только раз в 2года. Так же важная составляющая это топливо. Его должно хватить для полета туда и обратно. Из-за малых технических возможностей взять с собой большой его запас невозможно. Вообще, топливо необходимо для преодоления земного притяжения и выхода на околоземную орбиту, а также для торможения ракеты при подлете к Марсу. Весь путь ракета летит по инерции. Проблему с топливом можно решить, сделав более мощные двигатели и освоив новые виды топлива.

Есть несколько концепций двигателей будущего: плазменные, термоядерные, ионные и двигатели, основанные на темной материи [2]. Но пока это только теоретические возможности, на практике их еще не использовали. И это только лишь одна проблема, на самом деле их десятки: подбор специалистов, строительство ракеты, расчет траектории полета и так далее.Так почему бы человечеству не объединиться для решения этих проблем?!

Основной причиной отсутствия сотрудничества является соперничество. Говорить о полном разъединении нельзя, ведь некоторые страны действительно взаимодействуют. Сейчас речь идет об объединении технологий и ресурсов, но желание быть первыми мешает, в какой-то степени, освоению космоса.

Сравним технический потенциал ракет разных государств. Первая ракета в нашем списке – это российская ракета Протон-М, сконструирована еще 50 лет назад, но является лучшим носителем, совершая 10-12 полетов год, в то время, как иностранные ракеты-носители не превышают 6 запусков[3].

Реактивная тяга у первой ступени равна 971,4 тс. Сравним следующие характеристики: полезную нагрузку и тягу.

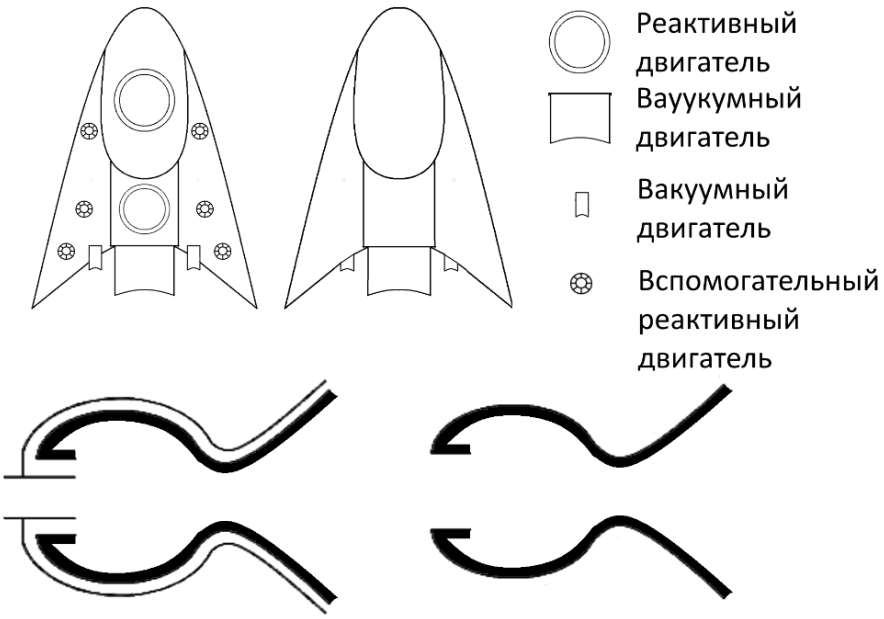
Дельта 4 – американская ракета носитель в тяжелой модификации, настоящий рекордсмен по массе выводимого на орбиту груза. Тяга равна 84,3 тс.

Ариан 5 принадлежит Евросоюзу. Изначально планировалась для совместного полета вместе с Геркулесом, но проект отменили и Ариан стал исключительно грузовой ракетой, которая имеет тягу 678,1 тс.

Можно составить рейтинг ракет носителей таких стран как Россия, США, Япония. На первом месте почетно расположился российский ракет носитель. У него самые лучшие показатели. Второе же досталось американской ракете. Третье место принадлежит японцам.

Предлагаем вам посмотреть наш проект ракеты будущего. Она имеет эллиптическую форму, которая обеспечивает обтекаемость. Так же есть 3 вакуумных двигателя, 2 реактивных, для большей эффективности есть еще 6 вспомогательных двигателей. Они подходят, как для преодоления сил притяжения, так и для вакуума.

В двигатель тоже вносим изменения. Предположительно, из-за дополнительного вращения слоя внутри камеры сгорания и сопла, ракета получит ускорение[1]. Следовательно, будет увеличена скорость, и топливо будет расходоваться меньше. Единственной проблемой, которую сложно решить, так это само топливо. Для долгих космических перелетов необходим генерируемый источник энергии. В данный момент ученые не могут решить эту задачу.



Итак, подведя итоги, можно сделать вывод о том, что бороздить космос не объединив усилия разных стран, очень затруднительно. Пока у человека нет возможности позволить

себе долгие космические перелеты. Но может быть, достаточно только объединиться и начать совместную работу!

Список использованных источников

1. https://ru.wikipedia.org/wiki/Жидкостный_ракетный_двигатель#:~:text=Форсуночная%20головка%20—%20узел%2C%20который,название%20этого%20узла%20«смесительная%20головка»
2. https://ru.qaz.wiki/wiki/Rocket_engine_nozzle
3. https://zen.yandex.ru/media/scienceeveryday/tipy-kosmicheskih-dvigatelei-kak-rabotaiut-rakety-i-chto-jdet-ih-v-buduscem-5c1960a97a772a00aaef036c?utm_source=serp
4. https://pikabu.ru/story/deystvuyushchie_raketanositeli_raznyikh_stran_kratkiy_obzor_2931372
5. https://asteropa.ru/istoriya-pokoreniya-kosmosa/#v-etap-issledovanie-planet-solnechnoy-sistemy

КТО ОН, ИЗОБРЕТАТЕЛЬ, ПОЛНОСТЬЮ ИЗМЕНИВШИЙ МИР?

Максюта Даниил Дмитриевич, студент 1-го курса
Научный руководитель Сергеева Наталья Александровна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Сегодня компьютеры проникли в повседневную жизнь людей настолько, что стали незаметными и люди уже не могут представить себе, как бы это могло быть по-другому. Поэтому назвать компьютер величайшим человеческим изобретением, кардинально и навсегда изменившим мир, не будет преувеличением, и актуальность этого очевидна.

Бесспорно, ЭВМ или, попросту говоря, компьютер – величайшее изобретение XX века. Но он возник не на пустом месте. Люди с давних пор пытались поручить выполнять сложные вычисления машинам. Первым механическим вычислительным устройством принято считать суммирующую машину гениального французского ученого Блеза Паскаля, создание которой началось еще в 1642 году. В 1808 году французский ткач Жозеф Мари Жаккард изобретает ткацкий станок, способный непросто производить ткань, а украшать ее произвольными узорами. Фактически это был программируемый станок. Узор задавался при помощи пластинок с дырочками, просверленными в определённом порядке – перфокарт. Мало кому известно, что в 1832 году русский изобретатель Семён Николаевич Корсаков публикует проект специальных машин для обработки информации при помощи перфокарт. Фактически, это были машины для работы с базами данных. Однако изобретение не получило официальной поддержки, комиссия, рассматривавшая проект, высказала мнение, что «Г-н Корсаков потратил слишком много разума на то, чтобы научить других обходиться без разума».

В 1834 году выдающийся английский математик Чарльз Бэббидж попытался построить универсальное вычислительное устройство – аналитическую машину, которая должна была выполнять вычисления без участия человека. Бэббидж не смог довести работу до конца – она оказалась слишком сложной для техники того времени. В 1991 году сотрудники Музея науки в Лондоне к 200-летию со дня рождения изобретателя воссоздали его машину, и она заработала. Машину Ч. Беббиджа называют праматерью компьютера, но до современных вычислительных устройств ей еще очень далеко.

К появлению первых ЭВМ привела целая череда открытий и изобретений в разных областях науки и техники: в химии, физике, электротехнике, математике и др.

Наиболее значимыми открытиями в области физики стали электричество и электромагнетизм. Об электричестве впервые упоминает греческий философ Фалес Милетский еще в VII веке до н. э., но термин *электричество* («янтарность») ввёл в обращение Уильям Гилберт только в 1600 году. Первую теорию электричества создаёт американец Бенджамин Франклин, который вводит понятие положительного и отрицательного заряда и доказывает электрическую природу молний. В 1791 году итальянец Гальвани описывает наличие электрического тока в мышцах животных, другой итальянец Вольта в 1800 году изобретает первый источник постоянного тока – гальванический элемент. **В 1820 году датский физик Эрстед доказал существование магнитного поля вокруг электрического тока.Опираясь на исследования Эрстеда, англичанин Майкл Фарадей в 1831 году открывает явление электромагнитной** индукции и **изобретает способ получения электрического тока.Анализ явления электролиза привёл Фарадея к мысли, что носителем электрических сил являются атомы как частицы материи. Открытие атома, теорию существования которого в 1803 году впервые представил англичанин Д.Дальтон, привело к развитию электронной теории.** В 1879 году американский изобретатель Томас Эдисон открыл явление термоэлектронной эмиссии, которое легло в основу создания в 1904 году английским физиком Дж. Флемингом диода – вакуумного

прибора, обладающего односторонней проводимостью электрического тока. Несколько позже был создан триод – лампа, в которой потоком электронов можно управлять с помощью третьего электрода – сетки.

Значимым открытием в области химии является появление ферритов, сочетающих магнитные свойства вещества с электрической полупроводимостью, которые применяются в электронике в качестве магнитных материалов. Их кривая намагничивания была впервые построена и исследована в 1878 году русским ученым А.Г. Столетовым.

С появлением полупроводников в первой половине XX века началась разработка интегральных микросхем, объединяющих в одном миниатюрном кристалле тысячи полупроводниковых приборов. В 1916 году русский ученый М.А. Бонч-Бруевич создал электронное реле, которое могло находиться в одном из двух состояний – 0 или 1 и на базе которого был создан триггер.

Успехи химии, физики и электротехники дали новый толчок в развитии средств передачи информации. Появление возможности использовать для передачи *информации* электрические сигналы привело к открытию новых направлений: радио, телеграфии, телефонии, а затем и телевидения.

В области математики объектом изучения в начале XX века стал алгоритм. Благодаря работам английского математика А.М. Тьюринга, американца Е.Поста, советских ученых А.А.Маркова и А.М.Колмогорова в середине XX века понятие алгоритма стало базовым понятием вычислительной техники. Сформировалось новое математическое направление – *алгебра логики*.В 70-х годах XIX века немецкий математик Г.Кантор выдвинул ряд идей, которые привели к созданию самостоятельной математической дисциплины – *теории множеств*. С развитием этой теории объектом алгебры логики стали функции и различные *операции* над ними. Практическое значение для вычислительной техники приобрел определенный класс функций, у которых значения равны всего двум величинам – 0 и 1, что соответствует двум логическим понятиям – «ложь» и «истина». Благодаря этой логике стало возможно конструирование логических схем.

Все эти открытия и изобретения послужили фундаментом для изобретения полноценной электронно-вычислительной машины.

Стимулом к созданию электронного компьютера стала Вторая мировая война, вовремя которой остро стояла задача быстрой расшифровкинемецкихсообщений. У англичан возникла проблема со взломомнемецких шифров: для этого требовалось огромное количество вычислений, и их нужно было сделать очень быстро, сразу после перехвата радиограммы. Для этого в Великобритании в 1943 году был построен мощныйэлектронныйкомпьютер «Колосс». Британское правительство рассматривало его проект как военную тайну на протяжении 30 лет, поэтому он не стал базой для дальнейшего развития компьютеров. Но это был первый в мире электронный цифровой компьютер.

К 1946 году американские ученые построилимощныйэлектронныйкомпьютер ЭНИАК, который содержал около 18 тыс. электронныхламп. Предполагалось, что его будут использовать для расчётов артиллерийских таблиц, которые выполнялись с помощью арифмометров и занимали много времени. ЭНИАК мог производить расчёты в 2400 раз быстрее человека с арифмометром. К моменту постройки компьютера острая необходимость в расчётах артиллерийских таблицо тпала, и компьютер стали использовать для других целей: для расчётов взрыва водородной бомбы, аэродинамики сверхзвуковых самолётов, прогноза погоды.

ЭВМ принято делить на поколения.Первое поколение настоящих ЭВМ на электронных лампах появилось в 1948 году. Для ввода программ и данных использовались перфокарты и перфоленты. Программы для таких машин составлялись на языках машинных команд. Это довольно сложно, поэтому программирование в те времена было доступно немногим.Скорость счета самых быстрых машин первого поколения доходила до 20 тыс. операций в секунду. Т.к. внутренняя память машин была невелика, то они пользовались для

инженерных и научных расчетов, не связанных с переработкой больших объемов данных. В СССР первая ЭВМ была создана в 1951г. и называлась она МЭСМ - малая электронная счетная машина. Конструктором МЭСМ был Сергей Алексеевич Лебедев.

Элементной базой машин второго поколения в 1959 году стали. Качество ЭВМ улучшилось по всем параметрам: они стали компактнее. надежнее, менее энергоемкими. Быстродействие большинства машин достигло десятков и сотен тысяч операций в секунду. Объем внутренней памяти возрос в сотни раз. Большое развитие получили устройства внешней (магнитной) памяти, благодаря этому появилась возможность создавать на ЭВМ информационно-справочные и поисковые системы. Во времена второго поколения активно стали развиваться языки программирования высокого уровня, программирование стало широко распространяться. Самым выдающимся достижением в 60-х г. XX века было изобретение БЭСМ-6 – это первая советская и одна из первых в мире ЭВМ с быстродействием 1 миллион операций в секунду.

Третье поколение ЭВМ охватывает период с конца 60-х по начало 80-х годов XX века. Его техническая база – интегральные схемы (ИС) или «микросхемы». Первые ИС содержали в себе десятки, затем – сотни элементов (транзисторов, сопротивлений и др.). Скорость работы наиболее мощных моделей ЭВМ достигла миллионов операций в секунду, появилась возможность выполнять одновременно несколько программ на одной машине. На них использовался новый тип внешних запоминающих устройств – магнитные диски, а также новые типы устройств ввода-вывода: дисплеи, графопостроители.ЭВМ третьего поколения – это система американских машин IBM-360 и машины серии ЕС ЭВМ в Советском Союзе. Существенно расширились и области применения ЭВМ: стали создаваться базы данных, первые системы искусственного интеллекта, системы автоматизированного проектирования и управления.

В 1971 году американская фирма Intel объявила о создании микропроцессора – это была революция. Микропроцессоры стали осуществлять управление работой станков, автомобилей, самолетов. Соединив микропроцессор с устройствами ввода-вывода, внешней памяти, получили новый тип компьютера – микро-ЭВМ – машину четвертого поколения. Их отличали малые габариты, большая надежность и сравнительная дешевизна. Это первый тип компьютеров, который появился в розничной торговле. Самой популярной разновидностью ЭВМ сегодня являются персональные компьютеры. Первый персональный компьютер серии Apple-1 появился на свет в 1976 г. под руководством американцев Стива Джобса и Стива Возняка. Программное обеспечение персонального компьютера позволяет человеку легко общаться с машиной, быстро усваивать основные приемы работы с ней, получать пользу от компьютера, не прибегая к программированию. Машины с такими свойствами быстро приобрели популярность, они постоянно совершенствуются и выпускаются большими тиражами.

Современный компьютер – это универсальное, многофункциональное, электронное автоматическое устройство для работы с информацией. Компьютеры проникли во все сферы деятельности человека и продолжают развиваться…

В мир компьютерных технологий постоянно приходят новые разработки, поражающие всё более совершенными и почти фантастическими модификациями. Сегодня уже выпущены компьютерные концепты, которые пока не вышли в серийное производство, но возможно уже скоро станут доступными миллионам пользователей по всему миру: компьютер без клавиатуры и дисплея, складной ноутбук с гибким дисплеем, который может сворачиваться как рулон бумаги, лэптоп с мембранной клавиатурой, гибкий раздвижной дисплей, наручный компьютер и многое другое. Насколько коммерчески успешным будут такие продукты сегодня – большой вопрос: для значительной части пользователей компьютеры сегодня заменили мобильные телефоны.

Более далекое компьютерное будущее может быть разным, и путей к нему тоже много, но ни то, ни другое предсказать невозможно. Однако в большинстве сценариев

прогресс приводит к изменению способа нашего общения, объема информации, с которой нам придется иметь дело, и, возможно, даже наших природных способностей.

О внешнем виде компьютера будущего можно только строить предположения. Однако, как говорил Лем, «будущее выглядит иначе, чем мы его себе представляем». С уверенностью можно сказать лишь одно – габаритные размеры систем будущего будут уменьшаться, а возможности и производительность значительно увеличатся.

По всему миру в различных лабораториях проводятся эксперименты по разработке принципиально новых вычислительных систем. В основе новых систем будут лежать нечто принципиально новое, а не кремниевые чипы. Это связано с тем, что современным компьютерам попросту дальше некуда развиваться. Мы уже скоро выйдем в нанотехнологиях на уровень атомов – и дальше двигаться некуда. Транзистор меньше атома пока построить невозможно. Можно увеличивать частоты, количество ядер, но все это временные меры. Только принципиально новые технологии обеспечат значительный рост производительности. Возможно, произойдет технологический скачок с тысячекратным увеличением мощности компьютеров.

К технологиям, способным многократно увеличивать обрабатывающую мощность компьютеров, можно отнести ДНК и другие биологические материалы, молекулярные или атомные, трехмерные, фотонные и квантовые технологии. Если на каком-нибудь из этих направлений удастся добиться успеха, то компьютеры могут стать вездесущими, а если успешных направлений будет несколько, то они распределятся по разным нишам.

Что касается функциональных возможностей компьютеров будущего, то ожидается, что они смогут воспринимать и обрабатывать изображение в режиме реального времени. Например, это даст возможность создавать системы контроля безопасности, которые анализируя окружающую их обстановку смогут предсказывать стихийные бедствия или теракты. Главное преимуществом такой системы– отсутствие усталости или потери бдительности. Кроме этого качественное «зрение» даст возможность компьютерам лучше взаимодействовать с человеком, лучше воспринимая их мимику и жесты. Будущие компьютерные системы научатся лучше слышать. При этом улучшится не качество приема звука, а способность компьютера анализировать звуковой ряд. Уже сегодня они умеют воспринимать речь, а в будущем им предстоит улучшить данный навык – научиться различать тончайшие интонации.Кроме этого, компьютер будущего обучат расшифровывать звуки, издаваемые животными. Улучшенная таким образом система будет способна, например, объяснить родителям причины плача грудного ребенка. На основе анализа звуков компьютер будет способен предупредить о возникновении поломки у различного оборудования.Ожидается и появление возможности передавать тактильные ощущения. Это станет основой для революции в онлайн-продажах: товар можно будет и рассмотреть со всех сторон, и предварительно «потрогать».

Мобильные устройства оснастить дисплеями с большими диагоналями просто невозможно, а проекционное оборудование далеко не всегда удобно использовать. Но можно задействовать VRD (виртуальные ретинальные мониторы). В данной технологии изображение будет проецироваться непосредственно на сетчатку глаза. Пользователю в данном случае будет казаться, что монитор «подвешен» в воздухе перед ним.Если проецирование изображения осуществляется только на один глаз, его можно будет видеть одновременно с окружающими объектами. При проецировании на оба глаза будут создаваться реалистичные и объемные изображения.

Завершающим этапом развития интерфейсов может стать непосредственная связь между человеческим мозгом и электроникой, причем для этого вживление чипа под кожу будет не обязательным.

Что касается более детальных прогнозов, то специалисты предсказывают, что уже в ближайшее время провода и кабели окончательно уйдут в прошлое, а компьютер достигнет вычислительной мощности человеческого мозга. К середине XXI столетия бессмертие станет потенциально возможным с помощью использования армии наноботов, дополняющей

иммунную систему и «очищающей» организм от болезней, благодаря изобилию нанороботов человеческий организм получит способность принимать любую форму, небиологический интеллект станет в миллиарды раз «умнее» биологического, и Земля превратится в один гигантский компьютер, а в мире киберпространства будут царить микро- и наноустройства (интеллектуальная пыль). К тому времени интернет будет представлять собой отображение всего реального мира, грань между кибер- и реальным пространством исчезнет.

Сегодня в такие прогнозы поверить достаточно трудно, сложно заглядывать вперед более чем на несколько лет, но можно с уверенностью сказать – компьютер будущего будет таким, каким мы его сейчас и представить не можем…

Человечеству пришлось потратить не один век, чтобы создать первую ЭВМ и дать однозначный ответ на вопрос «Кто изобрёл компьютер?» практически невозможно. Как и в случае со многими другими открытиями, мы обязаны этим величайшим достижением великим умам – ученым, изобретателям и ремесленникам, которые в разное время и в разных странах открыли явления, придумали и создали приборы и механизмы, на базе которых и строится современный компьютер.

Список использованных источников

1. Кто изобрёл компьютер? [Электронный ресурс]. - URL:http://kakizobreli.ru/kto-izobryol-kompyuter/(дата обращения: 09.02.2021).
2. Кто придумал компьютер? [Электронный ресурс]. - URL: https://yandex.ru/turbo/xn--e1adcaacuhnujm.xn--p1ai/s/kto-pridumal-kompyuter.html/(дата обращения: 15.02.2021).
3. Первая патентная война, или Кто изобрел компьютер[Электронный ресурс]. - URL: https://itc.ua/articles/pervaya-patentnaya-voyna-ili-kto-izobrel-kompyuter/(дата обращения: 03.03.2021).

ПСИХОГЕОМЕТРИЯ, КАК ПРОЕКТИВНАЯ МЕТОДИКА ИССЛЕДОВАНИЯ ТИПОЛОГИИ ЛИЧНОСТИ

Макшанова Елена Дмитриевна, студентка 1-го курса,
Сергеев Михаил Александрович, студент 1 курса,
Научные руководители Маликова Светлана Анатольевна,
преподаватель первой категории, педагог-психолог высшей категории,
Ковалёва Лариса Дмитриевна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Почему мы поступаем именно так, а не иначе, выбираем ценности, придерживаемся стиля в межличностных отношениях? Для эффективного общения с людьми, надо знать людей. Надо знать их психологию, возможные реакции и тогда легче планировать свои действия, слова, вообще отношения. Чтобы в учебной группе образовался слаженный коллектив, который будет успешно решать любые задачи, необходимо построить фундамент отношений. Существует много различных методик, направленных на изучение личности. В последнее время в психологических исследованиях и особенно диагностике часто используются графические методы.

Познакомившись с учебным предметом – геометрией - наукой о фигурах и их свойствах, возник проблемный вопрос «Находит ли геометрия свое воплощение в психологии, есть ли связь геометрических фигур и поведение людей?»

В основу работы положена гипотеза: попытки разделения разнообразия личностей на психологические типы по геометрическим фигурам.

Цель исследования: определение типа личности и их индивидуальных особенностей

Актуальность: данная работа позволит узнать больше о психогеометрии и проверить интуицию учащихся, чтобы знать, как с ними обращаться с данной информацией, взаимодействовать друг с другом.

Задачи:

- познакомиться с литературой по психогеометрии;
- познакомиться с методом изучения личности с помощью психогеометрии;
- провести исследование в виде эксперимента по изучению особенностей характера и распознаванию значений обучающимися.

Предмет исследования: проективный метод исследования личности.

Объект исследования: слушатели научно-исследовательской конференции.

Новизна: тема интересна тем, что позволяет быстро, без применения сложных тестов, определить психотип человека по особенностям его поведения, речи, одежде и манерам для того чтобы иметь возможность предположить возможные реакции личности на обстоятельства.

Для решения поставленных задач применили теоретический метод и проективную методику исследования личности «Психогеометрия», которая была разработана американским психологом Сьюзен Деллингер.

Но сначала маленький эксперимент с учебной группой МЧМ-20 - у психологов есть шутка, которая наглядно показывает, как ведут себя представители пяти психотипов по психогеометрии:

«Подошло пять автобусов, в которые надо рассесться представителям всех 5 фигур. Все будут вести себя по- разному:

- Круги – полезли в автобус весело, балагуря, подшучивая друг над другом, расселись по трое на сидениях, в результате, их влезло больше, чем надо.

- Треугольники – каждый пытался отодвинуть другого, и сели они по одному, стараясь занять лучшие места в начале автобуса и четко по одному на два сидения, в результате, их поместилось в два раза меньше, чем было мест в автобусе.

- Квадраты –дисциплинированно вошли, аккуратно расселись, четко выполняли указания, доставили меньше всего хлопот.

- Прямоугольники – их пришлось загонять в автобус, кто-то боялся войти, кто-то потерялся на станции, кто-то не знал, как входить и просил разъяснить ему, на их рассадку ушло больше всего времени.

- Зигзаги – полезли в автобус всеми способами, кто-то через окно, кто-то через люк в крыше, расселись тоже, кто во что горазд, стали давать советы водителю, как лучше вести автобус, начался обмен идеями, что можно в этом автобусе усовершенствовать».

Эта шутка наглядно и быстро показывает все пять психотипов, которые созданы Сьюзен Деллингер. Она назвала свою теорию – психогеометрия, именно потому, что все ее психотипы ассоциируются с одной из основных геометрических фигур.

В результате анализа проведённого эксперимента каждого человека в группе, можно сказать о том, что каждый 4 верно ассоциирует фигуры с текстом

Среди опрошенных группы МЧМ-20 разделяются таким образом: в большинстве случаев интуитивно определяют верно значение каждой фигуры до ознакомления со значениями теста по 25%, большего всего людей угадывают фигуру зигзаг, а меньше всего квадрат, путая его часто с кругом.

Мы изучили психотипы по их интерпретации в тесте:

Квадрат, например – это труженик, представители этого типа любят планировать, и он не любит изменения привычного хода событий. Такие люди опрятнывнешне, речь медленная, их позы напряжённые, а походка медленная, мимика практически отсутствует.

Треугольники - это лидеры. Они энергичные, ставят ясные цели идостигают их, не любят быть неправыми и с большим трудом признают свои ошибки. Выглядят так:одеваются ярко, речь быстрая, походка энергичная, жесты уверенные,мимика выразительная.

Прямоугольник - это люди, не довольные тем образом жизни, который сложился, поэтому находятся в поиске лучшего положения, они имеют низкую самооценку, стремятся стать лучше в чем-то, ищут что-то новое. Внешний вид не экстравагантный, в большой степени зависимый от того «что нашлось в гардеробе».

Круги – это хорошие слушатели, обладают эмпатией, не любят конфликтов,стремятся к общению. Поза у такого человека часто расслабленна, на лице улыбка, мягкая походка, мимика богатая и миролюбивая.

Зигзаг- символизирует творчество. Они не любят ограничения и рамки, любят разнообразие и свободу, они бывают несдержанныи эспрессивны.

Внешний вид часто бывает демонстративным, даже неряшливым, речь яркая, быстрая, позы часто меняются, жесты оживлённые, мимика живая.

Проведя исследования по изучению особенностей характера, мы можем применить знания и в жизни:

Выслушивать квадрата до конца, и не перебивать, обосновывать своё мнение фактами и цифрами. Воздерживаться от эмоциональных проявлений.

С треугольником необходимо говорить только по делу, четко и уверенно. Договариваться, а все спорные моменты треугольник трактует в свою пользу.

Прямоугольника необходимо поддерживать и направлять своим вниманием и влиянием.

Мягко, но настойчиво возвращать к сути дела необходимо с последователямикруга. Быть готовым к тому, что круг пообещает, но не сделает (ему легче согласиться с вами, а потом «как-нибудь все обойдется»).

Зигзаг... Повлиять на зигзага практически невозможно. Всегда следует быть готовым к резким сменам решений и тем разговора.

Изучая выбранную тему, мы узнали много нового, интересного из истории геометрии, о происхождения названий некоторых фигур, также научились диагностировать себя с помощью графических тестов, что является очень важным. Работа была увлекательной и познавательной. Цель и задачи, которые были поставлены в начале работы, успешно достигнуты. Мы узнали об одном из способов деления людей на психологические типы, научились определять с помощью психогеометрии особенности характера людей. Но главное, теперь мы можем применять эти знания в жизни.

Выводы, которые мы сделали изучив методику:

1. Исследование личности с помощью психогеометрии позволяет быстро и точно нарисовать психологический портрет оппонента, узнать какие черты его характера являются главными, а какие – второстепенными;
2. Работа позволила лучше понять себя и других людей. Мы надеемся, что те знания, которые получили, будут способствовать более успешному общению с людьми как дома так и в колледже.
3. Так же заметили, что типы характера в чистом виде встречаются крайне редко, в каждом человеке обычно присутствует несколько типов. Стало понятно, почему с одними ребятами легко общаться, а с другими – нет, почему возникают ссоры, конфликты и как можно решать проблемы.

Вывод: большинство людей интуитивно знают о резкой фигуре зигзаге, думают о том, что квадрат – это веселый человек, спокойный и не конфликтный, и всё это человек думает по сути не осознано, угадывая фигуры. Но есть люди, которые мыслят и думают по-своему, неверно оценивая фигуры.

Так же можно сделать вывод о том, что люди могут часто ориентироваться на выборе своего соседа, по типу: что выбрал он - выберу и я (это видно по результатам проведения эксперимента). Многие учащиеся - доброжелательные, заинтересованные в хороших отношениях, высшая ценность для них – благополучие окружающих, также это люди с развитой интуицией, устремленные в будущее. Это видно на примере экспериментальной группы, кто сидели рядом, написали практически одни и те же фигуры в одном и том же варианте.

Список использованных источников:

1. Алексеев А.А., Громова Л.А. Психогеометрия для менеджеров – « Знание»., 1991.
2. Психогеометрическое тестирование (теоретический и практический аспекты) – Авторы Козача В.В., Гарбер Е.И. – Самара, 2002.

АНАЛИЗ ЦЕЛЕВОГО РЫНКА СЕМЕЙНОЙ КОФЕЙНИ

Мальцева Евгения Николаевна, студентка 3-го курса
Перехода Анжелика Романовна, студентка 3-го курса
Научный руководитель Василевская Галина Николаевна,
преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС»,
г. Старый Оскол

Для любой бизнес-идеи необходимо провести анализ целевой аудитории, чтобы понять реализуема ли она. Семейная кофейня - для родителей и детей, совмещённая с продажей игрушек. В процессе поиска поставщиков игрушек через посредников поняли, что либо рынок перенасыщен, игрушки у всех повторяются, либо товары имеют не маржинальную стоимость.

Целевая аудитория в основном пары с детьми и девушки с мужчинами. Минимальный возраст клиента 18 лет, а максимальный бывает разный от 65 и более. Нашими клиентами являются, работающие люди, имеющие достаточный доход.

Девушки от 18 до 30 лет – живущие в близь лежащих районов и имеющие средний и высокий доход. Предпочитают капучино и мягкие игрушки. Мужчины в возрасте от 18 до 30 лет, работающие – живущие в близь лежащих районов и имеющие средний и высокий доход. Предпочитают американо. Семьи с детьми – живущие в близь лежащих районов и имеющие средний и высокий доход. Предпочитают мягкие игрушки, а также пить чай и сладкие напитки.

Сегментирование рынка – это с одной стороны метод для нахождения частей рынка и определения объектов, на которые направлена маркетинговая деятельность предприятия, а с другой стороны это управленческий метод принятия решений.

Объектами сегментации являются потребители продукции.

При сегментировании рынка товаров народного потребления обычно учитываются географические, демографические, социально-экономические, психографические, поведенческие признаки.

В нашем случае при сегментировании преобладает демографический критерий.

Рисунок 1- Полученные сегменты

1 сегмент: первая возрастная категория – девушки от 18 до 30 лет – живущие в близь лежащих районов и имеющие средний и высокий доход.

2 сегмент: мужчины в возрасте от 18 до 30 лет, работающие – живущие в близь лежащих районов и имеющие средний и высокий доход.

3 сегмент: мужчины и женщины 30+ с детьми – живущие в близь лежащих районов и имеющие средний и высокий доход. Предпочитают разнообразные игрушки, а также пить чай и сладкие напитки.

Покупатели и потребители – семьи с детьми, женщины и мужчины.

Услуга направлена на модель продаж в секторе B2C.

Businessto Consumer – это схема коммерческого взаимоотношения, где в качестве покупателя выступает конечный потребитель.

Применение метода 5 «W» Марка Шеррингтона:

Что? (What?) Кофе и игрушки.

Кто? (Who?) Семьи с детьми, доход средний-выше среднего, следят за собой, интересуются модой, живут в ближайших домах.

Почему? (Why?) Хотя приятно провести время в уютной атмосфере, хотят похвастаться перед друзьями и в социальных сетях.

Когда? (When?) Каждый день/неделю/месяц.

Где? (Where?) При просмотре страниц в соц. сетях. При прогулке по улице.

Для выявления потребностей проводился опрос в GOOGL форме: https://docs.google.com/forms/d/e/1FAIpQLSc-u0bvTagwTlzGGZWaFif73kr2Gq-brKXvq-Pd6XpDRaHlAQ/viewform.

Результаты опроса:

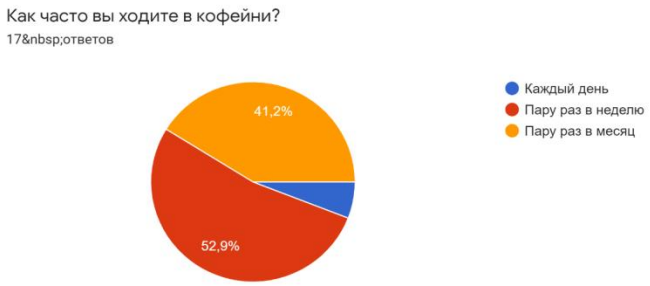


Рисунок 2 – Частота посещения кофейни

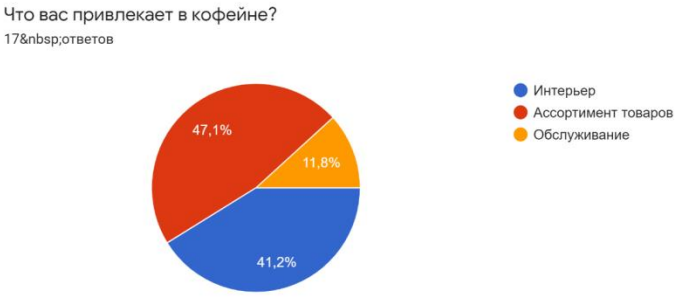


Рисунок 3 – Что привлекает покупателей

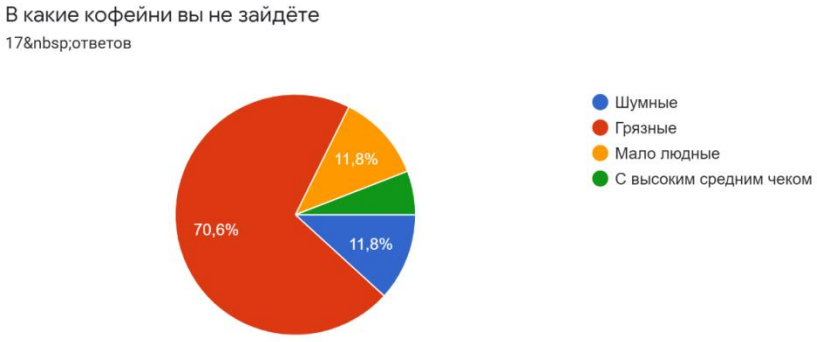


Рисунок 4 – Что отталкивает покупателей

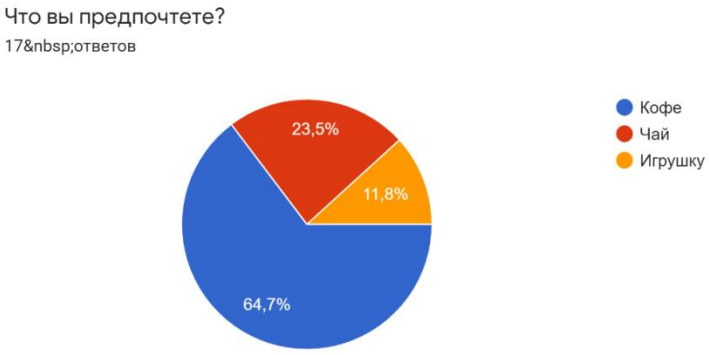


Рисунок 5 – Что больше предпочитают покупатели

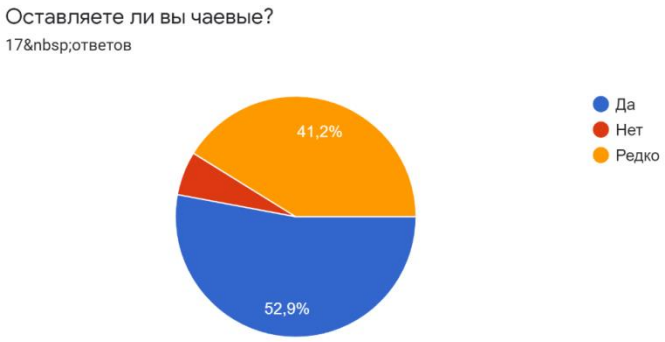


Рисунок 6 – Частота чаевых

Необходим аутсорсинг. Прежде чем открывать кофе с собой с нуля, в бизнес-плане необходимо продумать концепцию развития и продвижение. Открыть кофейню с нуля (самостоятельно).

Позитивные моменты реализации бизнес-идеи: использование недорогой аренды помещения, постоянно расширяющийся рынок, актуально для современного рынка.

Негативные моменты реализации бизнес-идеи: высокая конкуренция в городе, несформированный имидж кофейни, возможная автоматизация услуги в будущем.

Список использованных источников:

1. Анискин Ю.П. Управление инвестициями: учеб. пос. для вузов. - 3 - е изд., стер. - М.: Омега - Л, 2019. - 192 с.
2. Михайлов А.А. Основные правила создания своего дела для начинающих предпринимателей - М: Просвещение, 2020.- 170 с.
3. Рыжих О.Н. «Легко ли быть предпринимателем?»- М.: Дрофа,2019.- 302 с.
4. Халтаева С.Р. Яковлева И.А. Бизнес – планирование: Учебное пособие – Улан – Удэ, 2018 . – 574 с.

ЭКОЛОГИЧЕСКАЯ ПОЛИТИКА АО «ОСКОЛЬСКИЙ ЭЛЕКТРОМЕТАЛЛУРГИЧЕСКИЙ КОМБИНАТ»

Мартынов Михаил Сергеевич, студент 3-го курса
Научные руководители Старых Галина Александровна,
преподаватель высшей категории, Козлова Лариса Михайловна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего профессионального образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Металлургическая отрасль находится на втором месте среди всех других отраслей промышленности по атмосферным выбросам. Предприятия черной и цветной металлургии при извлечении металлов вынуждены использовать руду с очень низким содержанием полезных компонентов. Таким образом, на обогащение и плавку поступает огромный объем руды, а это, в свою очередь, порождает большиеколичества отходящих газов из неиспользуемых компонентов. Именно загрязнение атмосферы является главной причиной экологических проблем, возникающих в результате деятельности металлургических гигантов. Выбросы из труб приводят к загрязнениям почв, уничтожению растительности и образованию техногенных пустошей вокруг крупных заводов. К тому же, экологические проблемы отечественной металлургии обостряются из-за высокого износа оборудования и устаревших технологий. По данным Минпромэнерго, до 70% всех мощностей в отечественной металлургической промышленности являются изношенными, устаревшими и убыточными

Цель исследования: проанализировать экологическую политику ОЭМК и его воздействие на окружающую среду.

Задачей выступает изучение информацию по защите и охране окружающей среды на АО «ОЭМК» и и анализ природоохранной деятельности предприятия.

Объект: Оскольский электрометаллургический комбинат.

Предмет: Природоохранная деятельность ОЭМК.

Гипотеза: Природоохранная деятельность АО «ОЭМК» соответствует требованиям законодательства РФ, международных стандартов, норм и правил в области охраны окружающей среды.

В своей работе АО «ОЭМК» руководствуется принципом неукоснительного выполнения требований законодательства Российской Федерации, международных стандартов, норм и правил в области охраны окружающей среды. Природоохранная деятельность комбината направлена на снижение отрицательного воздействия на окружающую среду.

ОАО «ОЭМК» является современным металлургическим предприятием. При производстве стали применена технология, основанная на прямом восстановлении железа с использованием природного газа, что позволяет получать металл с минимальным негативным воздействием на окружающую среду. В проекте ОАО «ОЭМК» реализованы передовые технологические решения по охране атмосферного воздуха.

Применение системы гидротранспорта для поставки железорудного концентрата исключает использование железнодорожного транспорта, операций погрузки и разгрузки. Процесс бесшумен, легко поддается контролю, регулированию и автоматизации, беспылен.

Использование для межцеховых и внутрицеховых транспортировок сырьевых и производственных материалов закрытых конвейерных систем и специального автотранспорта позволяет исключить загрязнение окружающей среды за счет исключения запыленности при транспортировке сырья.

Все основные технологические агрегаты обеспечены пылегазоочистыми установками. В настоящее время в подразделениях ОАО «ОЭМК» эксплуатируется 97 пылегазоочистных

устройств. Существующее пылегазоочистное оборудование обеспечивает эффективность очистки от пыли в пределах 90-99%.

Очистка газов от пыли, в основном, сухая – электрофильтры (10 шт.), тканевые фильтры (53 шт.), циклоны (14 шт.) и только с целью снижения пожароопасности пыли, за некоторыми системами предусмотрена установка мокрых систем очистки газов – скруббера (20 шт.) (на системах транспортировки металлизованных окатышей в ЦОиМ, ЭСПЦ). Ряд установок имеют двухступенчатые очистки: пылевая камера и электрофильтр (за вращающимися печами ЦОИ); циклон и электрофильтр, (мельница, сушильный барабан бентонита в ЦОиМ), циклон и тканевый фильтр (шлифовальные станки в ЭСПЦ, шлифовальные машины в СПЦ-1), батарейный циклон и мокрый скруббер (участок шихтоподачи в ЭСПЦ).

Важнейшей целью в области природоохранной деятельности комбината является снижение и предотвращение отрицательного воздействия на окружающую среду в процессе производственной деятельности, обеспечение необходимой защиты здоровья и безопасности работников комбината и в близлежащих населенных пунктах. Для этого в бюджете предприятия в 2012 году на охрану окружающей среды было инвестировано 1560,424 млн. руб., в том числе на модернизацию газоочистки ДСП-150 №1-4 было затрачено 965,088 млн. руб. из них на завершение работ по первому модулю - 908,109 млн. руб.

На комбинате разработан проект нормативов предельно допустимых выбросов (ПДВ), получено разрешение на выброс загрязняющих веществ в атмосферный воздух.

ОАО «ОЭМК» постоянно осуществляет систематический производственный контроль за выбросами загрязняющих веществ в атмосферу и эффективностью работы пылегазоочистных сооружений, в соответствии с графиками аналитического контроля технологических выбросов и атмосферного воздуха от основных источников ОАО «ОЭМК» и графика проверки эффективности работы пылегазоочистных сооружений. Пылеочистные установки работают эффективно. Выбросы загрязняющих веществ не превышают норматив ПДВ.

Еженедельно, в соответствии с утвержденным графиком контроля, отбираются пробы воздуха на территории комбината, на границе СЗЗ, в близлежащих населенных пунктах, а также дополнительно производится отбор проб атмосферного воздуха в городе, в парке кинотеатра «Быль».

В настоящее время выполнен отчет по результатам проведения годового мониторинга, получено экспертное заключение по результатам санитарно-эпидемиологической экспертизы материалов по установлению размера единой СЗЗ и получено предварительное заключение Управления Роспотребнадзора по Белгородской области.

Список использованных источников

1. ОЭМК им. А.А. Угарова // Металлоинвест. Ресурсы создают возможности. URL: https://www.metalloinvest.com/business/steel/oemk/(дата обращения: 18.03.2021).
2. Гусев А.М., Афонина Е.А., Черчинцев В.Д. Разработка системы регенерации рукавных фильтров // Теория и технология металлургического производства: межрегион. сб. науч. тр. Вып. 6. Магнитогорск: ГОУ ВПО «МГТУ», 2006. С. 198 - 201.
3. Теория и практика ведения локального экологического мониторинга окружающей среды меднорудных горно-металлургических комплексов / А.И. Семячков, Л.П. Парфенова, В.А. Почечун, О.А. Копенкина. Екатеринбург: Институт экономики УрО РАН, 2008. 226 с.

ПОИСК КЛИЕНТОВ ЦЕНТРА ЛИЧНОСТНОГО РОСТА С ПОМОЩЬЮ МЕТОДА 5 «W» ШЕРРИНГТОНА И ВОРОНКИ ПРОДАЖ

Мезенцева Елизавета Александровна, студентка 3-го курса
Овчинникова Алла Сергеевна, студентка 3-го курса
Научный руководитель Василевская Галина Николаевна,
преподаватель высшей категории
Старооскольский технологический институт им.А.А.Угарова (филиал) Федерального государственного автономного образовательного учреждения высшего образования "Национальный исследовательский технологический университет "МИСиС",
г. Старый Оскол

Одной из распространенных идей для бизнеса на современном рынке являются Центры личностного роста, услуги которых востребованы коммерческими и образовательными организациями.

Прибегнув к методу 5 «W» Марка Шеррингтона можно подробно ответить на 5 вопросов своих клиентов. Данный метод помогает учесть практически все решающие факторы для создания предложения, интересного для клиента и выбора способов продвижения товара или услуги.

Для оценки количества заинтересованных лиц был проведен опрос в социальных сетях.

Воронка продаж – это известный маркетинговый инструмент для планирования и оценки эффективности бизнеса, позволяющий выявить слабые этапы бизнеса для их дальнейшей ликвидации (рисунок 1).

Полученная воронка показывает, что основные потери клиентов происходят на начальном этапе, т.е. кол-во узнавших и увидевших очень мало и незначительно, особенно по сравнению с объемом целевого рынка, наша задача – правильно спланировать маркетинговый план, дабы привлечь наибольшее число покупателей.

Таблица 1 - Метод 5 «W» Марка Шеррингтона

	Вопрос	**Ответ**
why?	Почему они обращаются в Центр личностного роста?	Потому что такого рода центры являются весьма редким явлением в нашем городе, но предоставляют: - **организациям** прекрасную возможность для дополнительного развития обучающихся или работающих в них лиц и налаживания коммуникаций внутри групп; - **отдельным людям** помощь в их внутреннем саморазвитии и самопринятии. **Главное преимущество** – высокая компетентность специалистов.
what?	Что мы можем им предложить?	Различного рода тренинги, способствующие всестороннему развитию и личностному росту, повышение экономической и юридической образованности людей неэкономических и неюридических специальностей.
who?	Кто наши клиенты?	- **Юридические лица,** приобретающие курсы для своих работников или учащихся, для их развития и повышения продуктивности; - **Физические лица**, приобретающие услуги для удовлетворения собственных потребностей.

when?	Когда они к нам приходят?	- Когда возникает возможность и желание поощрить активных студентов или работников, помочь наладить коммуникацию в группах, повысить работоспособность, помочь им в их социализации и профориентации. - Разобраться в себе, найти силы, мотивацию, свое предназначение, получить навыки общения, взаимодействия, самоанализа и повышение продуктивности.
where?	Где можно приобрести услугу?	Через социальную сеть **ВКонтакте**: *https://vk.com/tvoy_shag31* , **Инстаграмм**: https://instagram.com/tvoyshag31?igshid=x8rusxdpwr00, а также по месту фактического нахождения. **Юридический адрес:** Белгородская область, г. Старый Оскол, м-н Макаренко, 3а, каб.212.

Рисунок 1 –Воронка продаж

Полученная воронка показывает, что основные потери клиентов происходят на начальном этапе, т.е. кол-во узнавших и увидевших очень мало и незначительно, особенно по сравнению с объемом целевого рынка, наша задача – правильно спланировать маркетинговый план, дабы привлечь наибольшее число покупателей.

Список использованных источников:

1. Анискин Ю.П. Управление инвестициями: учеб. пос. для вузов. - 3 - е изд., стер. - М.: Омега - Л, 2019. - 192 с.
2. Михайлов А.А. Основные правила создания своего дела для начинающих предпринимателей - М: Просвещение, 2020.- 170 с.
3. Рыжих О.Н. «Легко ли быть предпринимателем?»- М.: Дрофа,2019.- 302 с.
4. Халтаева С.Р. Яковлева И.А. Бизнес – планирование: Учебное пособие – Улан – Удэ, 2018 . – 574 с.

ИССЛЕДОВАНИЕ ХИМИЧЕСКОГО ЗАГРЯЗНЕНИЯ АТМОСФЕРНОГО ВОЗДУХА

Прусов Артем Антонович, Ханчалян Завен Степанович, студенты 2 курса
Научный руководитель Умеренкова Татьяна Ивановна, преподаватель высшей категории
Старооскольский технологический институт им. А.А.Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж,
город Старый Оскол

Всем известно, что жизнь любого человека начинается с дыхания, а заканчивается с его прекращением. Человек может какое то время обходиться без еды, без воды, но не дышать он не может.

Стремительный рост численности человечества и его научно-технической вооружённости в корне изменили ситуацию на Земле. Современная цивилизация осуществляет невиданное воздействие на природу. Загрязнение природной среды промышленными выбросами оказывает вредное воздействие на людей, животных, растения, почву, здания, сооружения, снижает прозрачность атмосферы, повышает влажность воздуха, увеличивает число дней с туманами и т. д. [1].

Загрязнение атмосферы является одной из серьезных проблем для всего человечества. На величину концентрации вредных примесей в воздухе влияют разные факторы: скорость и направление ветра, температурные инверсии, которые препятствуют развитию вертикальных движений воздуха и способствуют образованию зон с повышенным содержанием примесей в приземном слое атмосферы.[4].

В данной работе мы оцениванием уровень загрязненности атмосферного воздуха в зимний и весенний период по химическому составу атмосферных осадков. Осадки накапливают в себе растворенные химические вещества, содержащиеся в атмосферном воздухе, поэтому являются индикатором его загрязнения.

Воздух никогда не бывает чистым. В нем всегда находится определенное количество примесей. Общая масса загрязнений, нависающих над планетой, составляет порядка 10 млн. тонн, что обусловлено процессами, происходящими в природе и производственной деятельностью человека. До 70% вредных выбросов приходится на долю автотранспорта. В выхлопных газах автомобилей содержится около 200 различных веществ, в том числе – углеводороды, оксиды углерода, азота, альдегиды, сажа и смолистые вещества [3].

Наиболее существенными источниками загрязнений сельскохозяйственных угодий являются минеральные удобрения и ядохимикаты. В промышленности основная масса вредных веществ, выбрасываемых в атмосферу, приходится на предприятия черной и цветной металлургии, нефтедобычи и нефтепереработки, стройиндустрии и теплоэнергетики[4].

Степень загрязнения атмосферного воздуха Старооскольского городского округа считается повышенной. Большая доля вредных выбросов в атмосферу приходится на объекты горнорудной и металлургической промышленности, а также на предприятия по производству стройматериалов. В сумме эти стационарные источники выбрасывают 67,8% от общего объёма загрязняющих атмосферу города веществ. Кроме этого, воздух Старого Оскола серьёзно загрязняется выхлопными газами автомобилей. Самыми крупными загрязнителями являются ОАО «Оскольский электрометаллургический комбинат», ОАО «Лебединский горно-обогатительный комбинат», ЗАО «Осколцемент», АО Стойленский горно-обогатительный комбинат». В промышленности по производству стройматериалов достигнуты высокие уровни очистки и утилизации твердых веществ, составляющие 97%. Большие объемы загрязнителей в атмосферу поступают от ЗАО «Осколцемент»: 1000 тонн угарного газа, 1700 тонн оксидов азота. Эти газы не улавливаются и не утилизируются.

Целью нашей работы явилось исследование химического загрязнения атмосферы в зоне промышленных предприятий города Старый Оскол. Объектом исследования выбран атмосферный воздух в районе промышленных предприятий: Стойленский ГОК и Осколцемент. Предмет исследования: катионно – анионный состав, тяжелые металлы, твердые загрязнители.

Задачи исследования: изучение методики обнаружения загрязнителей атмосферного воздуха; определение катионно – анионного состава, концентрации тяжелых металлов и массы осаждающихся твердых загрязнителей атмосферных осадков; обработка и анализ результатов исследования. Использовались методы исследования: качественный анализ и визуальное наблюдение, количественный анализ.

Исследование проводили в зимнее и весеннее время. Для исследования химического загрязнения атмосферы брали пробы атмосферных осадков в зоне Стойленского ГОКа и Осколцемента.

По результатам качественного анализа атмосферных осадков видно, что ионы Fe^{2+} присутствуют во всех пробах и преимущественно в количестве 1-6 мг/л. Ионы трехвалентного железа присутствуют не во всех пробах и в меньшем количестве, чем ионы двухвалентного железа. В большинстве проб концентрация ионов Fe^{3+} в районе Стойленского ГОКа достигала 0,4-1,0 мг/л. Большую концентрацию железа в атмосфере этого предприятия можно объяснить присутствием железа в ископаемом сырье. Белгородская земля богата железом.

Катионы кальция присутствуют во всех пробах атмосферных осадков. Это и естественно: около города находятся меловые карьеры. В большем количестве они присутствуют в районе предприятий Осколцемент и Стойленский ГОК, их концентрация здесь достигает 100 мг/л. Строительные соединения, содержащие кальций – это мел и известь.

Присутствие сульфат-, нитрат - и нитрит- ионов свидетельствует о наличии в атмосфере соответствующих кислотных оксидов, которые имеют преимущественно антропогенное происхождение. Сера входит в состав всех видов топлива. При работе промышленных печей, котельных, двигателей внутреннего сгорания сера выделяется в атмосферу в виде сернистого газа, который при дальнейшем окислении превращается в оксид серы (VI), который при взаимодействии с атмосферной влагой образует серную кислоту. При дальнейших химических реакциях в атмосфере образуются различные сульфаты и возникают сульфат-ионы SO_4^{2-}[2].

Аналогичным образом образуются нитрит - и нитрат - ионы. Основными источниками оксидов азота являются автотранспорт и сжигание топлива. Причиной образования оксида азота являются высокотемпературные процессы обжига на предприятиях стройиндустрии и других предприятиях. Образующийся при этом оксид азота (II) далее окисляется в атмосфере в диоксид азота, который при взаимодействии с атмосферной влагой образует азотную и азотистую кислоты: $2NO_2 + H_2O = HNO_3 + HNO_2$. Эти кислоты могут образовывать соответствующие соли. При диссоциации этих кислот и соответствующих им солей образуются ионы NO^{3-} и NO^{2-} [2].Частично серная и азотная кислоты используются для зачистки изделий в металлообработке и на предприятиях. В результате, в атмосфере этих предприятий присутствуют газы SO_2, NO, NO_2.

Концентрацию тяжелых металлов в атмосферных осадках, собранных в зоне промышленных предприятий города Старый Оскол, определяли комплексонометрическим методом. Определение тяжелых металлов позволило установить присутствие цинка в атмосфере предприятий.

Сравнительная оценка показала, что наибольший вклад в загрязнение атмосферы нашего города твердыми веществами вносят предприятия, связанные с производством цемента и асбестированных изделий. Их вклад в 2-6 раз больше по сравнению с другими предприятиями.

Проведенное исследование позволило сделать следующие выводы:

1. Атмосфера Старооскольского городского округа загрязнена такими химическими элементами, как кальций, железо и цинк, особенно в зоне промышленных предприятий.

2. Присутствие в исследуемых образцах сульфат -, нитрат – и нитрит–ионов свидетельствует о наличии в атмосферном воздухе оксидов серы и оксидов азота.

3. Наиболее запыленной является атмосфера в районе промышленного предприятия «Осколцемент».

4. Промышленные предприятия оказывают сильное влияние на качественный состав атмосферного воздуха, чем ухудшают условия жизни населения Старооскольского городского округа.

В результате проделанной работы выяснили много полезных сведений об атмосфере и ее состоянии. Она является защитным экраном от губительного воздействия космоса. Необходимо принимать меры, способствующие уменьшению загрязнения атмосферы: использовать безотходные технологии, экологически чистые виды энергии, производить очистку атмосферных выбросов, добиваться уменьшения токсичности автомобильных выхлопных газов.

Большая часть экологических проблем является общей для любого региона. Однако различные промышленные предприятия имеют свою специфику производства, свой «набор загрязнителей» атмосферы. Все это требует исследования и принятия соответствующих мер реагирования.

Список использованных источников

1. АшихминаТ.Я. Школьный экологический мониторинг:Учеб.пособие для учителей и учащихся/Под ред. Т.Я.Ашихминой. – М. : «Агар»:Рандеву-АМ, 2000. -386с.
2. Голдовская Л.Ф.Химия окружающей среды. – М.:Мир, 2005.-296с.
3. https://www.livelib.ru/book/1001221376-sledim-za-okruzhayuschej-sredoj-nashego-goroda-911-klassy-shkolnyj-praktikum-svetlana-mansurova
4. 4.https://bookree.org/reader?file=478157

Секция 1.4

ПОВАРЕННАЯ КНИГА МАТЕМАТИКИ

Майкова Ксения Федоровна, Щуров Андрей Владимирович, студенты 1-го курса
Научный руководитель Боровская Ираида Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

Все мы прекрасно знаем, что математика присутствует во многих сферах в нашей жизни. Но как насчет кулинарии? Есть ли там математика? Представляем вашему вниманию, кулинария с точки зрения математики!

Мы знаем, что для приготовления любого блюда должен соблюдаться рецепт. В рецепте берется точное соотношение продуктов, которое необходимо соблюдать в процессе приготовления. Математические величины масса и объём используют при взвешивании продуктов. Еще нужно помнить о единицах времени. Берем рецепт какого-либо блюда, например, борща с говядиной, нужную нам формулу и проводим сложные математические вычисления. В нашем случае мы не будем учитывать графу уксус и перец, потому что они по вкусу.

Но с другой стороны, математика — это точная наука, а в кулинарии нет никакой точности, каждый чувствует все по-своему и продукты не могут быть полностью одинаковыми. В этом и главная проблема.

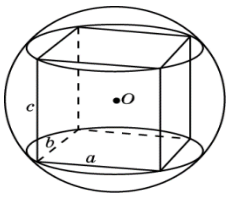
Но тут стоит вспомнить, что математика — это не только сложные алгебраические вычисления, но и так же геометрические. Геометрия уже больше подходит к кулинарии, не правда ли?

Геометрия очень сильно преобладает в кулинарии: в нарезке овощей для приготовления супов, салатов, вторых блюд, десертов.

Так же не с точки зрения эстетичности блюда, а по большой части правильного усвоения и приготовления пищи.

Но вопрос в том, какие формулы или законы надо применить, чтобы приготовить настоящий шедевр? На самом деле сейчас нам понадобятся лишь формулы для параллелепипеда. Возьмем для примера один из них.

В прямоугольный параллелепипед вписана сфера.



Вот его формула площади полной поверхности, объёма, радиуса вписанной сферы:

$$S = 6 \cdot a^2; \quad V = a^3; \quad r = \frac{a}{2}.$$

И так, мы имеем многогранник формулы к нему, можно найти его объём и радиус вписанной сферы.

А давайте приготовим идеальный геометрический десерт с помощью наших вычислений?

Хорошо, отойдем от темы кулинарии и ближе рассмотрим пропорции. Казалось бы, пропорции – одни из самых простых вещей в математике, да это так, но все намного глубже.

Приготовленные блюда нужно правильно делить на порции, в чём нам опять же помогает математика. Для того чтобы пользоваться кулинарными рецептами и производить перерасчет продуктов по ним, порой требуется знать, что такое отношение, пропорциональность.

«Вообще-то, незначительные детали обычно важнее всего» - сказал Шерлок Холмс[1]. Пропорции являются маленькой деталькой в большом механизме. Как мы уже знаем, пропорции есть везде и это значит, что пропорции являются неотъемлемой частью всего. Означает ли это, что благодаря пропорциям можно сделать много великих вещей? На самом деле пропорция – это больше инструмент для тех великих вещей. Это доказывает ее важность, и ее неотъемлемость.

Еще одно неожиданное применение пропорции мы нашли в музыке. Ученные проанализировали композиции великих музыкантов и установили, что в них присутствуют законы золотого сечения.

Сложно придумать сферу, где вообще не присутствует или хотя бы частично присутствует математика.

Даже наше с вами восприятие красоты основаны на математических пропорциях или по другому в золотом сечении.

Подытожив все выше сказанное можно сделать вывод о том, что математика, в каких-то ее проявлениях все-таки присутствует в кулинарии и абсолютно каждый может в этом убедиться. Математика – это многогранная наука, присутствие ее в многих сферах нашей жизни очевидно, только надо немного присмотреться.

Список использованных источников

1. Здобнов А.И. Сборник рецептов блюд и кулинарных изделий. – М.: Лада, 2010
2.Лысенко Е.А., Тонких А.П. Занимательная математика. – М.: Просвещение, 2006
3. Перельман Я.И. Как сделать изучение геометрии интересным и жизненным? // Математика в школе. 2008г.

Интернет источники

1. https://citatnica.ru/citaty/tsitaty-iz-filma-sherlok-holms-200-tsitat
2. http://heerdjaws.blogspot.ru/2012/11/blog-post_4119.html
3. http://www.magic-cook.com/forum/viewtopic.php?p=1766
4. http://www.workchild.30nar-s2.edusite.ru/ovosch/narezannie_ovoshi.html
5. https://math.wikireading.ru/2268

ПРОБЛЕМА СОВЕРШЕНСТВА ЧЕЛОВЕКА В ТЕОРИИ ПАССИОНАРНОСТИ Л.Н. ГУМИЛЕВА

Майкова Ксения Федоровна, студент 1-го курса
Научный руководитель Брендель Виктория Петровна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

Ключевые слова: человек, совершенный человек, сверхчеловек, герой, личность, ноосферный человек, «пассионарии», пассионарная теория, этнос.

Аннотация: Статья посвящена философско – психологическому осмыслению пассионарности – ключевого понятия пассионарной теории Л.Н. Гумилева. Конкретизируется этимология термина. Обосновывается, что пассионарии характеризуются высокой общей психической активностью и эмоциональностью. Уровень пассионарности оказывает влияние на направленность личности. Рассматриваются идеи совершенства человека в философском дискурсе. Обращается внимание на то, что в истории философской мысли формировались разные представления о совершенстве человека, рождались новые концепции, теории, идеи. На основе компаративного философского анализа, исследуется идея совершенства личности через понятия «совершенный человек», «сверхчеловек», «ноосферный человек», «пассионарная личность».

Человек, взятый в отдельности, а также рассматриваемый в родовой и социальной совокупности – есть проблема. Сколько людей – столько проблем, исходя из того, что раз нет человека - нет и связанных с его существованием проблем. И на протяжении всех времен и веков губили людей по одиночке и миллионами.

Тысячи лет человек выступает объектом научного и вненаучного знания. Прогресс сделанный учеными в различных областях науки, полученных в ходе проведенных исследованиях данных о человеке вновь и вновь требуют своего изучения и объяснения. Такова особенность любой науки: решая одни проблемы, она одновременно отрицает или плодит другие, расширяя границы и пределы исследований. В человеке остается много загадочного, скрытого и таинственного. Действия человека не поддаются рациональному истолкованию и адекватной оценке даже с помощью существующей теории, и методологии. Человек остается тайной, а происхождение человечества и его эволюции, условия его существование загадкой из загадок. Сократовский тезис – призыв «Познай самого себя» в полной мере не реализован, не смотря на все достижения в философии, психологии, медицине, биологии, этики, логики. Есть ряд ученых, полагающих, что проблема человека вообще не разрешима. В чем скорее был прав Ф.М. Достоевский «Человек есть тайна. Её надо разгадать, и ежели будешь разгадывать всю жизнь, то не говори, что потерял время…» [8].

Так кто же он, человек? В чем его сущность? Действительно ли она непознаваемая «вещь в себе» (И. Кант) и универсальна как «мера всех вещей» (Протагор)? Что есть биологическая и социальная природа человека? Каковы его эволюционные истоки и жизненные силы, социальные идеалы и система ценностей?

Идея совершенства личности, являющейся образцом для подражания, начала формироваться в античное время. Первоначально представления о «сверхчеловеке» соотносились с мифологическими героями и полубогами, в христианстве отождествлялись с Иисусом. С легкой руки Ф. Ницше, сформулировавшего понятие «Ubermensch» [7], в европейской философии родился концепт «сверхчеловек», который рассматривается как «комплексная, междисциплинарная и полиметодологическая тема» [8].

У Ф. Ницше идея «сверхчеловека» родилась как цель, объединяющая всех людей, в отсутствии у человечества единой морали. Он уверял, что только через обращение в

«сверхчеловека» можно освободиться от закрепощения моральными установками и предрассудками. Мыслитель призывал человечество на пути возвышения до «сверхчеловека», отказаться от существующих ценностей и от христианско-демократических идеалов. Ницше считал, что сверхчеловек должен быть свободным от нравственных ограничений, и наделён чувством превосходства, дающим ему власть над людьми. Достичь уровня «сверхчеловека» возможно при условии уничтожения внутри себя «твари» и взращивания «творца», что дано немногим [7].

Образ, созданный мыслителем, вызвал много споров и критику общественных отношений, вызов традиционной морали, христианству. Представители русской философско-религиозной мысли Н. Бердяев, В. Соловьев увидели в сверхчеловеке Ф. Ницше воплощенную идею зла, антихриста. Соловьев утверждал о опасности, грозящей христианской культуре, поэтому он создал противоположный «сверхчеловеку» образ «подлинного Богочеловека - Иисуса Христа, победившего смерть[9]. Н. Бердяев рекомендовал освятить божественным ореолом тех, кто проявляет в себе сверхчеловеческое[1]. П. Успенский, рассматривая человека как космическое существо, утверждал, что человек, являясь «господином вселенной», через идею самопреодоления способен достичь уровня сверхчеловека [10].

В разное время в философской мысли формировались разные представления о совершенстве человека, рождались новые концепции, теории, идеи. Абсолютно новым подходом к осмыслению идеи совершенства человека стала идея «ноосферного» человека, которая в последние годы приобретает особую актуальность. Научная база этой теории была заложена Н. Федоровым, В. Вернадским, и др. Ноосферой Вернадский называл сферу, рационально управляемую людьми, в создании которой участвует «коллективный разум людей, творческие идеи и замыслы личностей, духовная энергия, созидательный труд народных масс, рациональные поступки людей, направленные на формирование духовности» [2]. Ноосферный человек - это личность, несущая особую ответственность перед человечеством, воспринимающая себя чувствами, разумом как бессмертную органическую частичку вечной жизни. Существование ноосферного человека должно поддерживаться совершенствованием умственного, физического, нравственного, социального здоровья, которое зависит от состояния природы. Потому главной целью человека является забота о сохранении биосферы. Ноосферный человек - это экологический человек, выстраивающий природосохраняющую стратегию на духовно-нравственных началах.

На основе идей В. И. Вернадского о всплесках биохимической энергии в космосе, Л. Гумилев вводит в научный оборот понятие пассионарии, пассионарная личность. Пассионарность при определенных историко-географических условиях, культурных традициях и этническом окружении, обеспечивает появление новых людей. Л. Гумилев исследует феномен поведения этих людей, стремящихся осуществить свои идеи, ценой собственной жизни и жизни других и, оставив след в истории.

Для пассионарной личности моральные оценки неприемлемы, но присущи такие черты, как гордость, стимулирующая стремление к власти и славе, тщеславие, побуждающее к творчеству; ревность, способная к жестокости. В пассионариях заложено много противоречий, они легко совершают подвиги и идут на преступления; они способны созидать новое, творить прекрасное и одновременно разрушать существующее; в них соседствует добро и зло. Гумилев различает семь стадий пассионарного напряжения. Первую он назвал фазой подъема, когда начинает рост пассионарного напряжения. Далее следует акматическая фаза, процесс стабилизация напряжения. На фазе надлома начинается снижение пассионарного напряжения. Инерционная фаза рассматривается как процесс снижения напряжения, в результате происходит укрепление власти, социальных институтов, накопление культурных и материальных ценностей. На пятой фазе обскурации растет численность субпассионарии и падает пассионарность. Следующая фаза регенерации представляет процесс восстановления пассионарности на короткое время. На завершающем

этапе в реликтовой фазе устанавливается пассионарное напряжение на самом низком уровне. На фазе обскурации (деградации) появляются «субпассионарии» - люди с отрицательной пассионарностью, не способные к созиданию, инертны, равнодушные, проповедующие жизнь для себя [3].

В отличие от них, люди, обладающие признаком пассионарности, совершают поступки, создают новое (новые этносы). Несмотря на их небольшую численность, своим примером могут поднять в бой (А.В. Суворов), рискуя собственной жизнью, потому они обречены на гибель. Под пассионарностью понимается способность индивида к сверхусилиям, к сверхнапряжению, которая проявляется в готовности пожертвовать собственной жизнью во имя мира и счастья. Л. Гумилев выделил три вида пассионарности. Высокую пассионарность он расценивал как рецессивный, слабый, подавляемый признак. Пассионарность, развивающуюся на уровне нормы, соотносится с личностью, находящейся в состоянии гармонии с окружающей средой. Пассионарность ниже нормы, рассматривалась как субпассионарность, как склонность к пассивности, паразитизму [4].

Л. Гумилев предложил девять уровней классификации по признаку пассионарности:

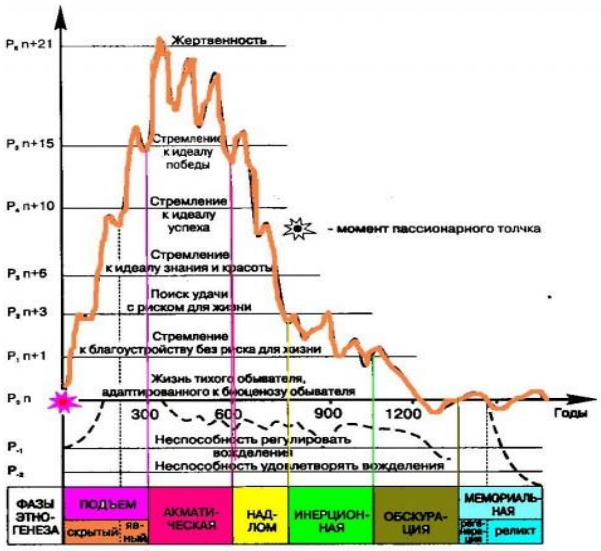


Рис.1. Уровни пассионарности

Таблица 1. Классификация по признаку пассионарности по Л. Н. Гумилеву

Уровень	**Название**	**Пояснинние**	**Описание**
6	жертвенный	высший уровень	человек без колебаний готов пожертвовать собственной жизнью. Примерами таких личностей являются Ян Гус,Жанна Д'Арк, протопоп Аввакум, Иван Сусанин
5			человек вполне готов рисковать жизнью ради достижения полного превосходства, но идти на верную смерть неспособен. Это патриарх Никон, Иосиф Сталин и др.
4	уровень перегрева / акматической фазы / переходный		То же самое что 5, но в меньшем масштабе — стремление к идеалу успеха. Примеры — Леонардо да Винчи, А. С. Грибоедов, С. Ю. Витте. Это
3	фаза надлома		стремление к идеалу знания и красоты и ниже (то, что Л. Н. Гумилёв называл «пассионарность слабая, но действенная»). Тут за примерами далеко ходить не надо — это все крупные учёные, художники, писатели, музыканты, и т. д.

2	поиск удачи с риском для жизни		Это искатель счастья, ловец фортуны, колониальный солдат, отчаянный путешественник, ещё способный рискнуть жизнью.
1			пассионарии, стремящиеся к благоустройству без риска для жизни
0	обыватель	нулевой уровень	тихий человек, полностью приспособленный к окружающему ландшафту. Количественно он преобладает почти во всех фазах этногенеза (кроме обскурации (время окончательной потери пассионарности)), но лишь в инерцию и гомеостаз является определяющим в поведении этноса.
-1	субпассионарии		ещё способны на какие-то действия, приспособление к ландшафту
-2	субпассионарии		не способны на действия, изменения. Постепенно с их взаимоистреблением и давлением внешних причин либо происходит гибель этноса, либо берут своё гармоничники (обыватели).

Существуют идеи о возможности создания «пассионарных реакторов», где пассионарность будет формироваться, расти, формировать пассионарных личностей. Анализируя современное общество, мы сделали вывод о том, что современное общество находится на фазе обскурации (деградации) в духовном плане, в нем преобладают субпассионарии, количество пассионариев минимально. Причина этого лежит в отсутствии идеи, в утрате традиционных ценностей, в пассивности и инфантильности современного поколения, в распущенности и вседозволенности. Большая часть современных людей не способны к созиданию, они инертны, равнодушны к проблемам общества.

В отличие от современного, в социалистическом обществе преобладали пассионарии. При наличии идеи построения коммунистического общества, сформировался огромный пласт людей, готовых пожертвовать собственной жизнью во имя светлого будущего. И в тот период сформировался новый образ «сверхчеловека», который был воплощен в образе героя, совершающего фронтовые и трудовые подвиги во имя Родины и своего народа. Основными ценностями героических людей были высшие социалистические ориентиры: долг, честь, героизм, патриотизм. Условием для роста пассионарности в социуме может стать война или революция. Рост таких личностей наблюдался в годы мировых войн, а в современном обществе - на территории Луганской и Донецкой народных республик[5].

Проблема совершенства человека на современном этапе развития общества приобретает особую актуальность и требует глубокого всестороннего исследования, так как в представлении масс он часто соотносится с образом «Киборга», «Бэтмена», «Робокопа», «Терминатора», обладающих сверчеловеческими способностями.

В последние годы появляются различные программы по «созданию сверхлюдей», ориентирующиеся на современные научные достижения: искусственный интеллект, генетику, генную инженерию, клонирование, робототехнику, нацеленные на создание человека, наделенного сверхспособностями. В отсутствие единого представления о совершенном человеке, совершенно очевидно, что ученые ориентируются на создание человека «технического», что приведет к вырождению человека «человеческого» [5].

Осмысление проблем современного общества подтверждает необходимость формирования совершенно нового типа человека, не «супермена», не «сверхчеловека», а личность, способную выстроить новый тип отношений с окружающим миром на основе рациональных знаний о себе, о природе, о вселенной. Собирательный образ совершенного человека должен соединить в себе лучшие качества ноосферной личности, пассионария, сверхчеловека, осознающего свое предназначение, умеющего оценить свои возможности, радикально изменить свое сознание, нацелить себя на достижение гармонии в духовной и обыденно-практической жизни, способного духовно преобразить себя и преобразовывать

окружающий мир. Он должен обладать сверхсознанием, которое на порядок превосходит сознание обычного человека, развиваться на уровне овладения современными научными знаниями, информационными технологиями. Совершенный человек - это высший тип человека, осознающий себя частью вселенной, несущий ценностный образец, задающий «рациональную меру» сознанию, словесной и деятельной практике, регулярно совершенствующий себя, развивающийся в единстве с миром, на основе духовных ценностей. Совершенный человек - это личность, способная и преобразовать окружающий мир, воспринимая его «глазами Бога».

Проблема сущности человека у Гумилева решается через соотношение природного и социального в человеке. Через понятия «этнос» и «пассионарность».

Теория евразийства, по мнению автора, даёт наиболее адекватное представление о человеке, проживавшем и живущем в России - Евразии.

Актуализация этнической составляющей в рамках теории Гумилева является проекцией евразийского вектора закрепления образов социально-исторической идентичности. Категории «пассионарность» и «этногенез» являются основополагающими для философско-культурологического выявления и определения специфических отличий динамики российского социума.

В результате проведенного исследования были решены следующие задачи: показан спектр решения проблемы человека в русском евразийстве. Раскрыт историософский смысл понятия «пассионарность». Охарактеризованы направления развития концепции пассионарности в современной философской антропологии. Сделаны попытки определить основные тенденции в дальнейшие разработки теории пассионарности. Рассмотрено развитие евразийского подхода к проблеме человека от истоков его формирования до современных научных и общественно- политических версий. При анализе научных трудов Л.Н. Гумилева, которые носят исторический характер выделен философский контекст, создана антропологическая реконструкция через неразрывную связь с этносом, определено понимание Гумилевым природы человека.

В завершении хочется отметить, что учение о пассионарности представляет собой большой интерес. Сама теория не содержит конкретных выводов, строится на размышлениях автора, что затрудняет исследование. А также тот факт, что труды Гумилева не были признаны в широких кругах, и обращение к его исследованиям возобновились недавно. Отвергать или полностью принимать положения ученого скорее нельзя, так как в них есть интересные, привлекающие внимание моменты. Человек, его происхождение – это «белое пятно» не только в исторической науке, почему именно философия, которая рассматривает эту проблему, может рассматривать е не в узком понимании, а совокупности с другими открытиями в разных областях науки.

Данная работа охватила лишь малую часть, и в дальнем автором будет продолжено исследование на более глубоком анализе.

Список использованных источников

1. Бердяев Н. А. Смысл истории. – М.: Мысль, 1990. – 177 с.
2. Вернадский В. И. Несколько слов о ноосфере // Вернадский В. И. Философские мысли натуралиста. – М.: Наука, 1988. – 520 с.
3. Гумилёв Л. Н. Этногенез и биосфера Земли. – СПб.: Кристалл, 2001. – 642 с.
4. Дмитревская И. В. Богочеловек В. Соловьева – Ноосферный человек. Прекрасный человек А. П. Чехова // Соловьевские чтения. – 2008. – Вып. 20. – С. 85–93.
5. Исаченко Н.Н. Идея «сверхчеловека» в философском дискурсе // Фундаментальные исследования. – Пенза: ИД «Академия естествознания». – 2014. - №11. – Ч. 9. – С. 86-89.
6. Ницше Ф. Сочинение в 2т. – Т.2 /перевод К. А. Свасьян. – М.: Мысль,1990. – 829 с.
7. Самохвалова В. И. Идея сверхчеловека в культуре [Электронный ресурс] – Режим доступа: htpp:// www.intelros.ru. (дата обращения: 07.04.16).

УЛЬТРАЗВУК

Маллер Карина Владимировна, Мулдашова Карина Руслановна, студенты 1-го курса
Научный руководитель Амельчакова Елена Анатольевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

Ультразвук – механические волны, подобные звуковым, но имеющие частоту от 20 килогерц до миллиарда герц.

Ультразвук начали изучать ещё в далёкой древности. Первые наблюдения были проведены в VI веке до нашей эры. Французский физик Поль Ланжевен впервые заметил повреждающее воздействие ультразвукового излучения на живые организмы. Итоги его наблюдений и сведения про то, что ультразвуковые волны могут проникать сквозь мягкие ткани человеческого организма, дали основания тому, что в 1930-х г. появился интерес к задаче использования ультразвука для терапии разнообразных заболеваний. В наше время ультразвук используется в различных физических и технологических методах.

Источниками ультразвука являются:

1 - излучатели-генераторы;
2 - электроакустические преобразователи;
3 - природные явления: звуки животного мира, естественные шумы;

В нашей природе ультразвук встречается как в качестве компонентов многих естественных шумов (в шуме ветра, водопада, дождя, в шуме гальки) и среди звуков животного мира. Некоторые животные используют ультразвуковые волны для обнаружения препятствий, ориентировки в пространстве и общения – это дельфины, грызуны.

Летучие мыши, применяют при ночном ориентировании эхолокацию, излучают при всем при этом ртом сигналы высокой интенсивности.

У ночных бабочек из семейства медведиц сформировался генератор ультразвуковых помех, «сбивающий со следа» летучих мышей, охотящихся на них.

Также эхолокацию используют птицы и китообразные.

Ультразвук применяется во многих сферах деятельности человека.

В области медицины

Современные ультразвуковые аппараты помогают врачам диагностировать и лечить широкий спектр состояний, травм и расстройств.

Самое распространенное использование ультразвука – это УЗИ. Оно позволяет получать данные об органах и визуализировать их.

Также ультразвук используют для лечения.

Ультразвук имеет такие действия как:

1- противовоспалительным, рассасывающим действиями;
2- анальгезирующим, спазмолитическим действием;
3- кавитационным усилением проницаемости кожи.

Но ультразвук может оказывать не только положительное влияние на организм человека, но и отрицательные действия. Чрезмерное воздействие этого высокочастотного звука может вызвать нарушения в работе нервной системы и сердечно-сосудистой системе.

В рыбной промышленности

В ней применяют ультразвуковую эхолокацию для обнаружения косяков рыб. Ультразвуковые волны отражаются от косяков рыб и приходят в приёмник ультразвука раньше, чем ультразвуковая волна, отразившаяся от дна.

В производстве

Ультразвук используется в резке металла. С помощью ультразвука возможно просверлить отверстия разных форм. Ультразвуком возможно делать винтовую нарезку в металлических деталях, в стекле, в рубине, в алмазе.

Ультразвук используют для очистки изделий. В лабораториях и на производстве используются ультразвуковые ванны для очистки лабораторной посуды и деталей от мелких частиц. В ювелирной промышленности ювелирные изделия чистят от мелких частиц полировальной пасты в ультразвуковых ваннах.

Также используется в ультразвуковой сварке. Это сварка давлением, исполняемая при воздействии ультразвуковых колебаний. Подобный вид сварки используется для соединения деталей, нагрев которых затруднён, при соединении разнородных металлов, металлов с прочными оксидными и для изготовления интегральных микросхем.

Вывод: в ходе исследовательской работы мы познакомились с теорией и историей ультразвука. Выяснили, где и как используется ультразвук, в каких областях он необходим.

Список использованных источников

1. https://school-science.ru Ультразвук и его пирменение в технике и медицине
2. https://rus-medteh.ru›uploads/MYeDITsINSKAYa AKUSTIKA…
3. https://бмэ.орг›index.php/УЛЬТРАЗВУК
4. https://cyberleninka.ru›Грнти›n/ultrazvuk-v-meditsine

СЕМЕЙНЫЕ ФОТОАЛЬБОМЫ В СОЦИОКУЛЬТУРНОЙ СИТУАЦИИ ПРОШЛОГО И НАСТОЯЩЕГО

Михайлов Илья Сергеевич, студент 2-го курса

Научный руководитель Канныкин Станислав Владимирович, доцент

Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

Актуальность работы обусловлена кризисным состоянием семьи как социального института. Одной из причин этого кризиса является межпоколенческая разобщенность, детерминированная резким ускорением социального времени и многоукладностью общественной жизни, которые значительно уменьшают возможности соприкосновения и взаимодействия разных поколений одной семьи. В этой связи большую значимость для сплочения родственников приобретает общая история малой социальной группы, одним из носителей которой выступает фотоальбом семьи.

Объект исследования: семейные фотоальбомы.

Предмет исследования: значимые семейные события, запечатленные на хранимых в альбомах фотографиях, а также их рецепция разными поколениями семьи.

Цель исследования: изучение особенностей ретрансляции биографической памяти поколений на примере семейного фотоальбома.

Задачи исследования: 1. Анализ научной литературы и интернет-источников по теме исследования. 2. Выявление наличных функций семейных фотографий. 3. Определение особенностей восприятия семейной истории посредством фотографий разными поколениями. 4. Исследование современных тенденций создания и функционирования в социальном пространстве семьи фотографий родственников.

Методы исследования: теоретический анализ научной литературы, сравнение, опрос, биографический метод, герменевтический метод.

В ходе анализа исследуемого домашнего архива семейных фотографий мы выяснили, что начало широкого распространения фотографирования членов семьи приходится на вторую половину XX века, что обусловлено возникшей доступностью фотоаппаратов и устройств для изготовления фотографий. Большая часть фотографий у представителей всех поколений является любительскими. Профессиональные изображения распространены на начальном этапе ведения альбома. История старшего поколения начинается с молодости, а среднего и младшего – с самого детства. Основным местом хранения большинства фотографий старшего и среднего поколения является бумажный альбом. Ведение альбома младшими поколениями прекращается в период средней школы, затем снимки размещаются в электронном формате.

Динамика в репрезентации поколений посредством фотографий связана с такими характеристиками, как изменение содержания фотографий (переход от постановочных снимков портретного жанра к бытовым, спонтанным и событийным; уменьшение количества фотографий, где изображены все члены семьи; появление «тематических» подборок или альбомов, как правило, связанных с поездками на отдых), повышение их качества (цветное фото), отражение на фотографиях семейных и социальных ролей (фото членов семьи, осуществляющих различные виды деятельности).

Анализируя влияние фотографии на память человека, мы пришли к выводу, что происходит вытеснение фотообразами образов-воспоминаний. С точки зрения молодого поколения основная функция фотоальбома заключается в сохранении семейной памяти. Представители старшей генерации воспринимают фотоальбом как одно из средств сплочения семьи, что достигается в процессе совместного просмотра. Среднее поколение выделяет для себя функцию документирования семейных историй и передачи их потомкам.

Также можно выделить информационную, консолидирующую, аккумуляционную функции и функцию визуальной ретроспекции связи времен и поколений.

Первоначально альбомы предназначались не только для хранения фотографий, но выступали в роли предмета декора. Богатое оформление в кожаном или бархатном переплете подтверждало статус владельца. Такие альбомы становились замечательным подарком, реликвией семьи, которая передавалась из поколения в поколение, и размещались на видном месте. Но важной функцией семейного альбома является осознание собственного места в семье, а семьи в обществе.

Рассуждая о функциях семейных фотоальбома, опрошенные в большинстве случаев называли функцию семейной памяти: «Память о том, как протекала жизнь раньше, как проходили праздники, встречи с друзьями, отдых и путешествия, и то, как меняется семья» (жен., 20 лет). В ходе опроса было выявлено, что распространенными функциями семейного фотоальбома являются функция семейной памяти, документирования семейной истории, ее ретрансляции следующим поколениям и консолидирующую функцию. Последняя заключается в том, что фотоальбом является способом объединения и укрепления семьи: «Совместный просмотр семейного фотоальбома. Это сближает членов семьи, напоминает им, сколько прекрасных моментов они пережили вместе» (жен., 20 лет). Действительно, часто в семьях на праздниках принято просматривать фотоальбомы в кругу близких и друзей.

В статье [8] авторы выделяют информационную, консолидирующую, аккумуляционную функции и функцию визуальной ретроспекции связи времен и поколений, что подтверждает наше исследование.

Можно определить различия в видении функционала семейного альбома у разных поколений. С точки зрения молодого поколения основная функция фотоальбома заключается в сохранении семейной памяти. Для представителей старшей генерации он служит для сплочения семьи, которое можно достичь в процессе совместного просмотра. Среднее поколение выделяет для себя функцию документирования семейных историй и передачи их потомкам.

По результатам нашего опроса, можно сделать вывод, что ведение и пополнение бумажных фотоальбомов постепенно прекращается. По сравнению с исследованиями, проведенными в 2009 – 2011 гг., такая тенденция стала выражаться гораздо сильнее. На вопрос «Ведется ли фотоальбом в настоящее время?» большинство респондентов ответили отрицательно или все реже: «Не ведется, так как сейчас все фото хранятся на цифровых носителях. Их всегда можно просмотреть на компьютере, не тратя время и деньги на распечатку» (жен., 20 лет). Если старшее поколение старается сохранять традицию ведения альбома, то младшее и среднее хранит фотографии в электронном виде. Такое решение объясняется тем, что привычные альбомы, как отмечают респонденты, имеют ряд недостатков: «таких как выцветание, то есть потеря первозданного цвета, что плохо влияет на качество передачи исходной информации. Следующий недостаток это их плохая сохраняемость вследствие того, что бумага довольно хрупкий материал. Электронные носители не обладают такими недостатками по этому я их и выбираю как основу моим фотографиям» (муж., 20 лет).

Актуальны ли фотоальбомы на сегодняшний день? На данный вопрос мнение у респондентов разделились. Часть считает, что фотоальбомы уходят в прошлое: «Я думаю, что привычные нам фотоальбомы теряют актуальность, потому что они подвержены старению. Все новые фотографии загружаются на цифровые носители, а только определенные попадают в альбом» (муж., 19 лет). Но большинство опрошенных указало на актуальность бумажного носителя: «Их актуальность в том, что в них мы размещаем только самые важные и лучшие снимки, то есть учимся отделять самое дорогое от незначительного, в то время как на цифровых носителях обычно огромное количество фото» (жен., 20 лет). Также актуальность объясняется эстетическими побуждениями, потому что такой фотоальбом можно подержать в руках, «ощущая тепло страниц».Такой альбом может

служить подарком: «Я считаю, что такие альбомы актуальны, ведь там собраны самые лучшие фото в одной тематике, можно дарить близким и показывать его гостям. Бумажных фотоальбомов не должно быть много, тогда они будут более ценными» (жен.,19 лет). При этом, отмечая недостатки хранения материала в электронном виде, опрошенные выделили опасность утраты таких фотографий в связи различными причинами: «Несмотря на технологическое развитие информационных носителей, бумажные фотоальбомы все равно остаются актуальными, т.к. фотографии в фотоальбоме могут хранится долгое время, а электронные файлы можно утратить по разным причинам, например, если электронный носитель сломается» (муж., 19 лет).

Несмотря на то, что большая часть респондентов считает фотоальбомы актуальными, их ведением занимается все реже. Это можно объяснить ускорением темпа жизни и сложностями поддержания бумажной семейной ценности. Мы хотели бы отметить важное достоинство электронных аналогов хранения - возможность цифровизировать бумажный альбом. Учитывая текущие тенденции, можно сказать, что в будущем ожидается полный переход фотоальбома на «новый уровень». Поэтому последующие исследования альбома как ретранслятора биографической памяти поколений будут совершенно иным.

По результатам нашего исследования выявлены тенденции уменьшения количества фотографий, отражающих печальные события в жизни семьи (фотографии похорон), постепенного прекращения пополнения бумажных фотоальбомов, усиление «развлекательной» функции фотографий и уменьшение их значимости, поскольку многие однотипные фото делаются в избыточном количестве и довольно быстро стираются из памяти цифровых устройств, освобождая место для новых фотографий.

Список использованных источников

1. Васильева Екатерина Витальевна, Стрельникова Анна Владимировна Биографическая память городских семей: опыт анализа фотоальбомов // Вестник РГГУ. Серия «Философия. Социология. Искусствоведение». 2012. №2 (82). URL: https://cyberleninka.ru/article/n/biograficheskaya-pamyat-gorodskih-semey-opyt-analiza-fotoalbomov-1 (дата обращения: 08.10.2020).
2. Гришкова Анастасия Андреевна Социальный смысл фотографии и эволюция семейного фотоальбома // Наука. Общество. Государство. 2016. №4 (16). URL: https://cyberleninka.ru/article/n/sotsialnyy-smysl-fotografii-i-evolyutsiya-semeynogo-fotoalboma (дата обращения: 08.10.2020).
3. Белова Д. Ю., Лысенко О. В. Повседневность через отражение семейного фотоальбома //Вестник научной ассоциации студентов и аспирантов исторического факультета Пермского государственного гуманитарно-педагогического университета. Серия: Studis historica juvenum. – 2012. – №. 1 (8).
4. Лишаев Сергей Александрович Помнить фотографией (к анализу фотографической конструкции памяти) // Вестник Самарской гуманитарной академии. Серия: Философия. Филология. 2009. №1. URL: https://cyberleninka.ru/article/n/pomnit-fotografiey-k-analizu-fotograficheskoy-konstruktsii-pamyati (дата обращения: 08.10.2020).
5. Лишаев С. А. Антропологические эффекты домашнего фотоархива //Перспективные информационные технологии. – 2016. – С. 1012-1016.
6. Печурина Анна Вячеславовна Увидеть необычное в обычном: исследования семейной фотографии // Социологический журнал. 2010. №2. URL: https://cyberleninka.ru/article/n/uvidet-neobychnoe-v-obychnom-issledovaniya-semeynoy-fotografii (дата обращения: 08.10.2020).
7. Гадарь Екатерина Викторовна Событийная структура памяти поколений: сравнительный анализ // Вестник РГГУ. Серия «Философия. Социология. Искусствоведение». 2011. №3 (65). URL: https://cyberleninka.ru/article/n/sobytiynaya-struktura-pamyati-pokoleniy-sravnitelnyy-analiz-1 (дата обращения: 08.10.2020).

8. Тельгузова В. А. Фотоальбом как способ консолидации семьи и визуальной ретроспекции межпоколенных связей //Актуальные проблемы развития человеческого потенциала в современном обществе. – 2018. – С. 300-303.

9. Зайцева И. А. Изображение и память: опыт культурологической интерпретации семейного фотоальбома //Национальное культурное наследие России: региональный аспект. – 2018. – С. 25-31.

10. Белова Д. Ю., Лысенко О. В. Изучение отдыха советских людей через семейный фотоальбом //Вестник научной ассоциации студентов и аспирантов исторического факультета Пермского государственного гуманитарно-педагогического университета. Серия: Studis historica juvenum. – 2013. – №. 1 (9).

11. Абилова Рамина Олеговна. Фотография как источник по изучению истории повседневности: анализ современной российской историографии: диссертация ... кандидата Исторических наук: 07.00.09 / Абилова Рамина Олеговна;[Место защиты: ФГАОУВО «Казанский (Приволжский) федеральный университет»], 2017.- 236 с.

12. Абилова Р. О. «Они всегда со мной»: к истории настенного фотоальбома //Вестник Чувашского университета. – 2015. – №. 4.

13. Чалфен Ричард Семейные фотографии как коммуникация посредством изображений // Социологический журнал. 2010. №2. URL: https://cyberleninka.ru/article/n/semeynye-fotografii-kak-kommunikatsiya-posredstvom-izobrazheniy (дата обращения: 08.10.2020).

14. Стрига Н. В., Петрова Л. Е. Диджиальная выставка семейных фотографий как механизм репрезентации городской повседневности //Цифровая культура открытых городов. – 2018. – С. 65-71.

15. Юмашева Ю.Ю. — Фотоархивы в сети Интернет: проблемы презентации и изучения // Историческая информатика. – 2019. – № 1. – С. 8 - 46. DOI: 10.7256/2585-7797.2019.1.29087 URL: https://nbpublish.com/library_read_article.php?id=2908710. (дата обращения: 08.10.2020).

16. История первого фотоальбома [Электронный ресурс] URL: https://www.fotoprizer.ru/articles/istoriya-fotografii/istoriya-sozdaniya-pervogo-fotoalboma/239/?q=1335&n=239 дата обращения: 08.10.2020).

17. Циттель, И. Философия семейного альбома [Электронный ресурс] / И. Циттель. – URL: http://big-turtle.ru/философия-семейного-альбома. (дата обращения: 08.10.2020).

МОДЕЛИ И МОДЕЛИРОВАНИЕ

Мишустина Алина Владимировна, студент 2-го курса
Научный руководитель Ткаченко Алла Юрьевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

По всем официальным и неофициальным рейтингам одними из наиболее востребованных на рынке труда являются специальности, связанные с IT-технологиями.

Самый важный этап разработки программного продукта – это построение модели. Таким образом в моей специальности моделирование – это одна из составляющих профессиональных компетенций. Поэтому считаю необходимым его изучение и области применения.

Цель работы: изучить понятия модель и моделирование.

Задачи:

- найти определение понятию модель и моделирование;
- найти информацию об области применения изучаемых на различных дисциплинах моделях.

Моделирование – процесс построения и использования модели. Под моделью понимают такой материальный или абстрактный объект, который в процессе изучения заменяет объект-оригинал, сохраняя его свойства, важные для данного исследования.

Моделирование используют, когда:

• *оригинал не существует:*
- древний Египет
- последствия ядерной войны (Н.Н. Моисеев, 1966)

• *исследование оригинала опасно для жизни или дорого:*
- управление ядерным реактором (Чернобыль, 1986)
- испытание нового скафандра для космонавтов
- разработка нового самолета или корабля

• *оригинал сложно исследовать непосредственно:*
- Солнечная система, галактика (большие размеры)
- атом, нейтрон (маленькие размеры)
- процессы в двигателе внутреннего сгорания (очень быстрые)
- геологические явления (очень медленные)

• *интересуют только некоторые свойства оригинала:*
- проверка краски для фюзеляжа самолета

Оригиналу может соответствовать несколько разных моделей и наоборот! Цель моделирования - понять и изучить качественную и количественную природу явления, отразить существенные для исследования черты явления (объекта, системы, процесса) в пригодной для использования в практической деятельности форме.

Модели также различают по области применения – это учебные, опытные, научно-технические

Модели могут представлять собой:

- Объект познания
- Средство познания

Существуют различные способы описания информационных моделей

1. Таблицы ;
2. Схемы;
3. Граф;
4. Блок-схема_.

Систему городских улиц удобно рассмотреть с помощью графов.

Схема проезда в метро наглядно покажет, как лучше проложить маршрут.

Так, на развитие химии и физики решающее влияние оказало создание Д. И. Менделеевым в конце XIX века периодической системы элементов, которая представляет собой табличную информационную модель.

На сегодняшний день самые популярные модели – 3d модели. В последние несколько лет 3D-печатные модели человеческих органов превратились в незаменимые атрибуты работы медиков разных сфер. Хирурги теперь могут заранее продумывать и даже полноценно отрепетировать ход проведения любых, даже очень сложных операций.

Вывод: из проделанной работы можно сказать, что модель – это упрощенное представление, аналог реального объекта, процесса, явления. Моделирование – это один из универсальных методов познания, состоящий в создании и исследования моделей. С помощью моделирования можно сделать объект более интересным и доступным для подробного изучения.

Список использованных источников

1. https://ktonanovenkogo.ru/voprosy-i-otvety/model-modelirovanie-chto-ehto-takoe.html
2. https://anrotech.ru/blog/3d-modelirovanie-v-sovremennom-mire/
3. https://ru.wikipedia.org/wiki/Моделирование
4. https://spravochnick.ru/informacionnye_tehnologii/informacionnye_modeli_i_modelirovanie/
5. https://www.zwsoft.ru/stati/imitacionnoe-modelirovanie-sistem-chto-eto-takoe-i-gde-ispolzuetsya

ПЕНСИОННАЯ СИСТЕМА КАК ОСНОВА СОЦИАЛЬНОЙ ПОЛИТИКИ ГОСУДАРСТВА

Моргунов Дмитрий Русланович, студент 1 курса
Научный руководитель Полупанова Ирина Ильинична, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Российская Федерация в соответствии со статьей 7 Конституции РФ является социальным государством, политика которого направлена на создание условий, обеспечивающих достойную жизнь и свободное развитие человека. Эти условия во многом обусловлены состоянием пенсионной системы, в частности, они зависят от размеров пенсий.

Социальная политика российского государства должна быть направлена на реализацию гражданином права на получение материального обеспечения в установленных законом случаях. Право на материальное обеспечение должно охраняться законом.

В Российской Федерации численность пенсионеров составляет более 43 млн. человек. Вся информация о них, а также иных потенциальных пенсионерах хранится в Пенсионном фонде РФ, органе назначающим и выплачивающим пенсии гражданам.

Обращение гражданина за пенсией является отдельной законодательно урегулированной процедурой, где обозначены как права и обязанности гражданина, так права и обязанности Пенсионного фонда РФ. В силу того, что данная процедура периодически меняется, представляется достаточно актуальным ее рассмотрение по действующему законодательству.

Россия вошла в рыночную экономику, унаследовав пенсионную систему СССР. При этой пенсионной системе пенсия гражданина, трудившегося всю жизнь, практически не зависела от размера его заработной платы и стажа работы. Платежи были обезличены и поступали в общую копилку, из которой они распределялись на выплаты пенсий.

Коренные изменения основ экономической жизни России в начале 1990-х гг. привели к изменению и принципов пенсионного обеспечения. Сегодня государственное пенсионное обеспечение основывается на обширной законодательной базе и имеет всеобщий характер.

Право на трудовую пенсию предоставляется всем гражданам, занятым трудовой или иной общественно полезной деятельностью. Гражданам, не имеющим по каким-либо причинам права на трудовую пенсию, устанавливается социальная пенсия на условиях и в порядке, который определяется Федеральным законом от 15 декабря 2001 г. № 166 ФЗ «О государственном пенсионном обеспечении в Российской Федерации».

Существует система пенсионного обеспечения, которая распределяется по группам. Первая группа - государственное пенсионное обеспечение. Государственной организацией, отвечающей за оплату пенсии, является Пенсионный Фонд Российской Федерации. Пенсия от государства передается гражданам из федерального бюджета, распределение ведется среди узких слоев населения.

Вторая группа - негосударственное пенсионное обеспечение. Данная система ведется частными Пенсионными Фондами и может быть индивидуальным и корпоративным.

Пенсия состоит из следующих частей: базовой (социальной), страховой и накопительной. Базовая (социальная), которая перечисляется государством без учета получаемого дохода (заработка) и величины взносов достигшим предусмотренного законом возраста и при наличии у претендента трудового стажа (минимум 5 лет).

Основной вид пенсии в России - это страховая пенсия по старости. До 2015 года она называлась трудовой, определяемой в зависимости от размера оплаченных в ПФ платежей за период ведения гражданином трудовой деятельности.

Помимо страховой пенсии есть накопительная, установленной с 2002 года и зависящей от аккумулированных отчислений, на которую могут претендовать лица,

родившиеся после 1953 года и 1957 года (мужчины и женщины соответственно). Средства накопительной пенсии, как следует из ее названия, формируются на индивидуальных счетах. Их ведет Пенсионный фонд (через частные управляющие компании или государственную - Внешэкономбанк) или негосударственные пенсионные фонды.

Целью государственного пенсионного обеспечения является начисление базовой части: пенсии по труду, пенсии по выслуге лет; по достижении пожилого возраста, по причине инвалидности; социальной пенсии. Законом Правительства, внесенным в Государственную Думу в июне 2018 года, предлагалось повысить общеустановленный пенсионный возраст на 5 лет для мужчин и на 8 лет для женщин, закрепив его на уровне 65 лет и 63 года соответственно.

В окончательном виде новый закон о пенсионной реформе был принят с учетом предложенных поправок 27 сентября 2018 года в третьем чтении. Уже 3 октября документ был одобрен Советом Федерации и подписан Президентом. Самой значительной поправкой Президента к этому закону является снижение нового пенсионного возраста женщинам на 3 года - до 60 лет вместо изначально предложенных в законопроекте 63 лет. Также Президент предложил льготные условия по выходу на пенсию в первые 2 года действия нового закона - в 2019 и 2020 гг. Все президентские поправки были одобрены депутатами в ходе чтения законопроекта в Госдуме.

Законодательные изменения в системе формирования и выплаты пенсии приводят к тому, что с одной стороны повышается срок выхода на пенсию, с другой – ее размер. Реформа во многом была вызвана большим процентом людей пожилого возраста в общем числе граждан, что связано с демографической ямой в связи с рядом событий новой и новейшей истории России. При этом те, кто сегодня работает и выплачивает взносы в ПФР, могут самостоятельно повлиять на увеличение своей пенсии, если воспользуются услугами негосударственных фондов.

Таким образом, законодательное обеспечение пенсий в РФ имеет довольно сложную и разветвленную систему, и еще не один год потребуется, чтобы её сбалансировать и заставить работать.

Список использованных источников

1. Блинов И. Пенсионная система России https://yandex.ru/turbo/vbr.ru/s/npf/help/chto-takoe-npf/pensionnaya-sistema-rossii/
2. Как устроена пенсионная система https://fincult.info/article/kak-ustroena-pensionnaya-sistema/
3. Пенсионная система Российской Федерации https://bankiros.ru/wiki/term/pensionnaa-sistema-rossijskoj-federacii
4. Что нужно знать о пенсионной системе https://pfr.gov.ru/grazhdanam/zakon/

ПРОЕКТНАЯ ДЕЯТЕЛЬНОСТЬ КАК ВОЗМОЖНОСТЬ СОТРУДНИЧЕСТВА С ПОТЕНЦИАЛЬНЫМИ РАБОТОДАТЕЛЯМИ

Пантрина Наталья Викторовна, студент 1-го курса
Научный руководитель Губарева Татьяна Викторовна, преподаватель
Автономная некоммерческая профессиональная образовательная организация «Национальный социально-педагогический колледж», г. Пермь

Трудоустройство выпускников по своей специальности на сегодняшний день является одной из актуальных проблем образовательных учреждений среднего профессионального образования. Решением этой проблемы может стать организация проектной деятельности студентов с привлечением потенциальных работодателей. Привлечение работодателей к участию в образовательном процессе, разработке профессиональных образовательных программ и оценке качества подготовки обучающихся к профессиональной деятельности является приоритетным в данном направлении.

Так, реализация образовательной программы по специальности 44.02.03 «Педагогика дополнительного образования» предусматривает порядок ее реализации с возможностью расширения и (или) углубления подготовки «для обеспечения конкурентоспособности выпускника в соответствии с запросами регионального рынка труда и возможностями продолжения образования». [1] Согласно требованиям к условиям реализации программы подготовки специалистов среднего звена «образовательная организация должна определить ее специфику с учетом направленности на удовлетворение потребностей рынка труда и работодателей, конкретизировать конечные результаты обучения в виде компетенций, умений и знаний, приобретаемого практического опыта».

Таким образом, работодатели формулируют требования как к количеству (целевой заказ), так и к качеству подготовки профессиональных кадров, а колледж удовлетворяет эти требования.

Анализ различных источников показывает, что основными направлениями совместной деятельности колледжа и работодателей являются:

- «определение требований к качеству подготовки специалистов (экспертиза основной образовательной программы, разработанной в соответствии с требованиями ФГОС СПО);
- включение в образовательный процесс дисциплин по рекомендациям работодателя для формирования интегративных свойств и качеств личности как наиболее значимых результатов образования, необходимых для дальнейшей профессиональной деятельности;
- организация учебной и производственной практик обучающихся на реальных рабочих местах производственного предприятия;
- расширение спектра образовательных услуг, востребованных на рынке труда;
- разработка и рецензирование учебно-программной документации;
- участие работодателей в государственной итоговой аттестации выпускников и промежуточной аттестации обучающихся по профессиональным модулям образовательной программы;
- стажировка на реальных рабочих местах;
- участие работодателей в научно-практических конференциях, учебных проектах, олимпиадах, конкурсах профессионального мастерства и т.д.». [2]

В связи с этим, выполнение проектных заданий в процессе прохождения различных видов практик у потенциальных работодателей приобретает особую значимость во взаимодействии колледжа и работодателей. Ведь, практика - это образовательный процесс, направленный на личное исследование и для педагогической практики такой опыт играет важную роль. Ведь в будущем, студенты будут иметь дело с детьми и подростками, а потому любое рабочее взаимодействие в данный период обучения под «присмотром» руководителей и работодателей является неоценимым опытом.

Организация проектной деятельности способствует реализации деятельностного подхода при прохождении практики и формированию у студентов профессиональных

компетенций (психолого-педагогической, методической, организационной, исследовательской и коммуникативной). В результате участия в проектной деятельности совместно с представителями работодателей студент овладевает навыками работы с временным детским коллективом; технологией проектирования; навыками управления проектами, методикой проведения занятий; методикой подведения итогов и сбора обратной связи. Конечно же, поиск информации, ее структурирование и оформление всей документации осуществляется посредством демонстрации студентом его навыков владения компьютерными технологиями.

Таким образом, выполнение практических заданий во время прохождения производственной практики обеспечивает приобретение обучающимися первого профессионального опыта работы и, тем самым, выступает в качестве «ведущего фактора, обеспечивающего эффективное формирование высокого уровня профессиональной компетентности будущих специалистов» [2].

Подводя итог, можно констатировать, что эффективность взаимодействия колледжа и работодателей в интересах повышения качества подготовки профессиональных кадров значительно возрастет, если удается осуществить перевод стратегических партнеров-работодателей из позиции сторонних наблюдателей и пассивных потребителей образовательных услуг в позицию заинтересованных участников образовательных и инновационных процессов, всемерно содействующих овладению обучающими комплексом профессиональных компетенций, отвечающих требованиям современного рынка труда, - именно такое сотрудничество способствует закреплению в производственных условиях знаний и умений, полученных при изучении профильных дисциплин, приобретению необходимых практических навыков.

Список использованных источников

1. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 44.02.03 Педагогика дополнительного образования (утв. приказом Министерства образования и науки РФ от 13 августа 2014 г. N 998). URL: http://ivo.garant.ru/#/document/70732836/paragraph/1:3.

2. Маралина И.А. Участие работодателей в образовательном процессе с целью приобретения профессиональных компетенций у обучающихся в рамках ФГОС СПО. - Электронный журнал «ПрофОбразование». - 2019. - Май. - 28. URL: http://проф-обр.рф/blog/2019-05-28-1379.

ГЕРОЙ-Я И ГЕРОЙ-ТЫ В АВТОРСКОМ ЛИРИЧЕСКОМ ТВОРЧЕСТВЕ

Разинкин Илья Сергеевич, студент 1-го курса
Научный руководитель Капустина Ирина Владимировна, преподаватель
Оскольский политехнический колледж Старооскольского технологического института им. А.А. Угарова (филиала) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», г. Старый Оскол

В молодости многие пишут стихи. Суть нашего исследования заключается в анализе собственного творчества – циклов стихотворений в прозе «Монологи о жизни» и «Приди-приди, рай…», опубликованных на личной странице в социальной сети ВКонтакте.

Актуальность работы мы видим в том, что в лирике молодых людей отражается мироощущение поколения конца XX-начала XXI века. Знакомясь с «Монологами…» читатель может легко реконструировать картину непростого временного периода жизни общества, может определить, чем живут типичные студенты-подростки в Российской провинции сегодня, какие чувства испытывают, как мыслят себя в обществе: «*Знаете, я вот всё чаще и чаще начинаю думать: а что сложнее - принять себя … Или же не принимать - работать, стараться, умнеть <….> Тяжело и дорого жить, но, как бы смешно это не звучало, умирать ведь тоже дорого, ведь это похороны это гроб, кладбище <…> Друзья которые тебе могут не верить, или же девушка которая может тебя не любить, нет не подумайте я не пытаюсь сейчас жаловаться на жизнь».*

По мнению М.М.Бахтина, Я и Другой предстают как два ценностных центра и три «мира» – пространство, время и смысл [1, с.78]. В моем творчестве это доказывают Прагматический аспект данного исследования заключается в том, что, во-первых, мы, студенты, узнаем лучше и больше друг о друге, учимся понимать и слышать другого, который Не-Я. А, во-вторых, новые читатели, в том числе и преподаватели колледжа, начинают лучше понимать нас, своих воспитанников, и мы для них не являемся тем, что можно определить как «другой». Первым шагом к Другому будет его увидение – замеченность, затем восприятие его телесности с окружением. Душа Другого – это внутренний мир человека, автора, отличное от соотнесенности Я своим собственным смыслом [1, с.114].

Я никогда не может воспринять себя целиком. Я видит лишь кусочки самого себя в пространстве. Даже когда Я смотрит на себя в зеркало, он видит себя со стороны, а не изнутри: *«Почему не придумали способ вернуть человека к жизни, придумали айфон, интернет всё угодно, почему не придумали лекарство от рака, или от другой не излечимой болезни... Что такое боль? <…> В детстве мои родители ссорились каждыми днями, потом отец ушёл, в школе и во дворе меня чмырили, а из двора вообще пытались выгнать: «Жырныййфуууйдиии».*

Говоря другими словами, «Монологи…» становятся своеобразным мостиком внутри «Поколения Z» и между поколениями, проводниками «духовного вещества» в среде «духовных существ».

В качестве литературоведческой основы нами использованы труды М.М.Бахтина, Л.Я.Гинзбург, Л.И.Тимофеева.

В целом, анализируя собственное творчество, мы можем сделать вывод о том, что молодые люди ощущают себя частицей человечества и мироздания. Подростки «Поколения Z» ищут пути выражения своих мыслей и чувств, способы понимания каждой личностью Другого, как «Ты - не Я» (то есть другого Я).

При этом автор драматично переживает как отчуждение других, так и возможность идентификации с ними.

Список использованных источников

1. Бахтин М.М. Автор и герой в эстетической деятельности // Бахтин М.М. Соч.: в 8 т. Т. 1. М., 2003. С. 69–264.
2. Бахтин М.М. Искусство и ответственность // Бахтин М.М. Соч.: в 8 т. Т. 1. М., 2003. С. 5–6.
3. Гинзбург Л.Я. О психологической прозе // Л.Я.Гинзбург. - [Электронный ресурс]. – Режим доступа: http://19v-euro-lit.niv.ru
4. Тимофеев Л.И. Слово в стихе // Л.И.Тимофеев. - [Электронный ресурс]. – Режим доступа: http://koob.ru

ПОТРЕБИТЕЛЬСКИЙ КРЕДИТ ИЛИ ИПОТЕЧНОЕ КРЕДИТОВАНИЕ
при покупке жилья – что выгоднее?

Репко Анатасия Андреевна, студент 3-го курса
Научный руководитель Зиннатуллина Анна Николаевна, преподаватель
Государственное автономное профессиональное образовательное учреждение
Уфимский топливно-энергетический колледж, г. Уфа

Согласно статистическим данным, по итогам 2020 года, Республика Башкортостан вошла в 10 регионов по России по вводу в действия жилых домов. При этом, каждый второй гражданин хоть раз задумывался над вопросом оформления кредита на покупку недвижимости.

Выбор формы кредитования зависит от разных факторов: официальное трудоустройство, уровень заработной платы, наличие первоначального взноса, возможность оформления субсидии и льгот. Помимо этого, проблема финансовой неграмотности среди разных слоев населения занимает ведущее место. Особенно эта проблема затрагивает молодых семей или граждан в пенсионном возрасте. [3]

Ежедневно, в средствах массовой информации мы можем увидеть или услышать об ипотеке или о кредите. И тогда, у нас возникает вопрос: а что выгоднее брать, кредит или же ипотеку?

Для начала разберемся, что же такое кредит и ипотека?

Понятие «кредит» существует на протяжении тысяч лет. Кредитные отношения в процессе своего становления видоизменялись в связи с изменением общественно-экономических отношений и прошли несколько этапов: зарождение, становление и регулирование.

Необходимость в кредитных отношениях стала появляться еще в момент начала разделения общества на бедных и богатых в период первобытной общины. На первых этапах «кредитования» кредитор не зарабатывал на том, что давал в долг, это была вынужденная мера, так как у более бедных была жизненная необходимость брать в долг, у них не хватало зерна и продуктов питания, они брали в долг в надежде, что на следующий год их урожай будет больше, и они смогут вернуть взятое. Наказанием за несвоевременную выплату кредита было лишение свободы, или рабство, где не отдавший долг был обязан трудиться на благо кредитора, только позднее компенсация за оказанную услугу стала имущественной (материальной). [1]

Ипотечное кредитование появилось сравнительно недавно, свое законодательное обеспечение получила лишь в 1998 году, когда вышел Федеральный закон №102- ФЗ « Об ипотеке». В общем виде ипотека – это залог недвижимого имущества, один из способов обеспечения исполнения обязательств, при котором закладываемый объект недвижимости остается во владении и пользовании должника, а кредитор, в случае невыполнения должником своего обязательства, приобретает право получить удовлетворение за счет реализации данного имущества. [2]

Несмотря на стремительное развитие ипотеки, потребительское кредитование остается ведущим продуктом, предоставляемый российскими банками. Только по итогам 2019 года, потребительское кредитование увеличилось на 2,7 % и составило 19,45 млн. единиц. Об этом говориться в сообщении Национального бюро кредитных историй (НБКИ).

В типичном сравнении этих двух банковских продуктов можно выделить плюсы и минусы.

В числе главных недостатков кредита называют следующие:

1. Кредит повышает реальную стоимость товара на сумму переплаты по нему. Особенно велика переплата по долгосрочным кредитам.
2. Кредит провоцирует лишние расходы, он увеличивает стоимость жизни дважды: за счет переплаты по процентам и за счет провоцирования необоснованных покупок.

3. Кредит со значительными выплатами ограничивает свободу на период его погашения, возрастают личные финансовые риски.

Плюсы кредитов также очевидны:

1. Кредит делает доступными дорогие, но необходимые предметы: жилье, авто и прочие.
2. Кредит улучает качество жизни, решает многие личные проблемы: оплата учебы, лечения.
3. Кредит помогает заработать: кредиты на бизнес, на инвестиции, на образование.

Плюсы ипотеки:

1. Процентная ставка по такому займу сравнительно невысока, существуют меры государственной поддержки населения.
2. Срок погашения кредита велик, что снижает ежемесячный платеж и делает кредит относительно необременительным;
3. Приобретенные страховки могут действительно оказаться полезными;
4. Используя ипотечную схему, заемщик получает право на налоговый вычет;
5. Соответствующая категория заемщиков может использовать такой финансовый инструмент как материнский капитал и существенно сократить тело кредита или первоначальный взнос.

Минусы ипотеки:

1. Оформление ипотечного займа - процедура долгая.
2. Клиенту потребуется купить страховку на приобретаемую недвижимость, а также застраховать собственную жизнь и здоровье.
3. У ипотеки существует минимальный размер. Очень многие банки неохотно предоставляют суммы меньше 500 тыс. рублей.
4. Приобретаемая квартира станет имуществом обремененным залогом. До тех пор, пока кредит не будет погашен, ее не получится продать или использовать для обеспечения по другому кредиту.
5. При совершении сделки клиенту нужно будет оплатить процедуру оценки недвижимости.
6. Банк выдаст кредит на покупку далеко не каждого объекта недвижимости. Заемщик ограничен в выборе будущего жилья.
7. Банки негативно относятся к тому, что в кредитной квартире будут прописаны несовершеннолетние дети или инвалиды. Это затрудняет реализацию обременения. [4]

Осуществляя свой выбор, покупатели жилья основываются на двух факторах – сложности получения денег и переплате по кредитному продукту. И если со стороны простоты получения средств безусловным лидером является нецелевой кредит, то с точки зрения того, что выгоднее ипотека или кредит на квартиру, ответ не очевиден.

На общую переплату влияет несколько факторов. Чем больше продолжительность действия договора – тем выше общая переплата. Сократить ее можно, оформив договор на более короткий срок, или погашая кредит на жилье досрочно.Однако предположить возможность погашения в более короткий срок бывает трудно. Каждые 5 лет ипотечного договора значительно увеличивают переплату. Лицам, которые не могут участвовать в программе льгот по ипотеке, и не могут получить налоговый вычет по какой-либо причине, стоит обдумать возможность оформления потребительского кредита. Отзывы что выгоднее кредит или ипотека среди заемщиков, с накоплениями более 70% от стоимости жилья, говорят о превосходстве потребительского кредита.

Семьям, ни разу не получавшим налоговый вычет, подходящим к программе Молодая семья, имеющим материнский капитал или члена семьи – военного, выгоднее будет оформить жилье в ипотеку. Выплаты от государства, льготная ставка, деньги от сертификата снизят кредитное бремя. Благодаря этому долг можно будет закрыть в более короткий срок, а значит, уменьшить переплату.

Также ипотека – самый подходящий вариант для лиц, которые не смогут платить большие ежемесячные платежи. Что выгоднее ипотека или потребительский кредит все же зависит от категории граждан. Однако из-за большего процента, начисляемого на остаток, при ипотеке, переплата будет меньше. [5]

Список использованной литературы

1. Деньги, кредит, банки: учебник / кол. авторов; под ред. засл. деят. науки РФ, проф. Лаврушина. – 9-е изд., стер. – М.: КНОРУС, 2017. – 560 с
2. Деньги, кредит банки. Денежный и кредитный рынки: учебник и практикум для среднего и профессионального образования / М.А.Абрамова(и др.); под общей редакцией М.А. Абрамовой , Л.С. Александровой.- 2-ое изд. испр. и доп. – Москва : Издательство Юрайт, 2020. – 436 с. – (Профессиональное образование).
3. Злодеева А.Е. – Ипотечное жилищное кредитование как часть экономической системы государства // Экономика, социология и право.- 2017.- № 11. – С. 10-12.

ЗАЧЕМ НУЖНА ПЕТЛЯ МЁБИУСА?

Строкаль Евгений Максимович, Толмачёв Илья Иванович, студенты 2-го курса
Научный руководитель Боровская Ираида Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

Некоторые научные знания и явления привносят в нашу жизнь тайну и загадку. Петля Мёбиуса относится к ним в полной мере. Мы интуитивно представляем, что такое "поверхность". Поверхность листа бумаги, поверхность стен аудитории, поверхность земного шара известны всем. Может ли быть что-нибудь неожиданное и даже таинственное в таком обычном понятии? Да! Это односторонняя поверхность. Пример такой поверхности – загадочный и великолепный лист Мёбиуса.

Мы знаем, как выглядит символ бесконечности, который напоминает перевернутую восьмерку. В переводе с древнегреческого языка бесконечность - это лента. Представьте себе, что символ бесконечности очень похож на реально существующую математическую фигуру. Знакомьтесь, Лента Мебиуса!

Открыл, эту таинственную ленту немецкий математик **Август Фердинанд Мебиус**, ученик великого Гаусса. Он написал много работ по геометрии, но славу ему принесла главным образом, эта поверхность. В 1858 году математик стал знаменит.

Эксклюзивность ленты заключается уже в том, что в отличие от обыкновенного листа бумаги она имеет только одну поверхность, а не две. Иными словами, если начать закрашивать лист бумаги, не переходя через грань, то закрасится только одна сторона. А лента Мебиуса закрасится с обеих сторон.

Лента Мебиуса – пример не ориентируемой односторонней поверхности с одним краем в обычном трёхмерном Евклидовом пространстве. Подавляющее большинство предметов имеют две стороны, например, лист бумаги. Чтобы поверить в то, что у петли Мебиуса всего один край – проведите пальцем по одному из граней ленты, не прерываясь, и Вы упретесь в точку, с которой начали движение.

Лента Мебиуса – вовсе не абстрактная фигура, необходимая только для целей математики, она используется и в настоящей обычной жизни. В соответствии с основными особенностями этого изобретения работает лента в аэропорту, движущая чемоданы из багажного отделения. Такая конструкция допускает ей служить дольше в связи с постоянным изнашиванием.

Также Лист Мёбиуса используют и в разных научных теориях. Например, существовала гипотеза, которую выдвинул советский цитолог Навашин, что форма **кольцевой хромосомы** по строению аналогична ленте Мебиуса.

Существует еще одна более значительная теория. **Вселенная – это гигантская петля Мебиуса**. Эйнштейн придерживался этой идеи. Он допустил, что Вселенная замкнута, и космический корабль, несущийся все время прямо, вернется в ту же самую точку в пространстве и времени, с которой и началось его движение.

Петля Мебиуса воодушевила художников на создание шедевров. Самой знаменитой является картина Moebius Strip II, Red Ants или Красные Муравьи голландского художника-графика Маурица Эшера.

По произведению «Лента Мёбиуса» писателя фантаста Армина Дейча снят не один фильм. В форме петли Мебиуса производится великое множество украшений, обуви, скульптур и других предметов.

Благодаря открытию Мёбиуса произошло улучшение свойств магнитных сердечников, изготовленных из ферро-магнитной ленты, намотанных по способу Мебиуса.

Н. Тесла запатентовал многофазную систему переменного тока, использовав намотку катушек генератора по типу петли Мебиуса.

Американский ученый Ричард Дэвис сконструировал нереактивный резистор Мебиуса - способный гасить реактивное (емкостное и индуктивное) сопротивление, не вызывая электромагнитных помех.

«Мышление начинается с удивления»,- заметил 2500 лет назад Аристотель. Наш современник Сухомлинский считал, «что чувство удивления – могучий источник желания знать: от удивления к знаниям – один шаг». А математика прекрасный предмет для удивления.

Именно это мы попытались показать в своей работе, описывая лист Мёбиуса и процесс его изготовления, раскрывая опытным путём свойства этого поразительного открытия. Наше предположение оправдалось, лента Мёбиуса обладает не только свойством односторонности, но и такими, действительно, непредсказуемыми свойствами, как связность и непрерывность.

На удивление, свойства ленты Мёбиуса применяются в самых различных изобретениях. Свойство односторонности листа Мебиуса было использовано в дизайне одежды и украшений, кулинарии, в химии, физике, технике, биологии. Если изготовить ременной передачи ремень в виде листа Мебиуса, то его поверхность будет приводиться в негодность вдвое медленнее, чем у обычного кольца. Это дает впечатляющую экономию. В матричных принтерах красящая лента также имела вид листа Мёбиуса для увеличения срока годности. В виде парадоксальной геометрической фигуры можно, оказывается, изготовить лопасти бетономешалки или обычного бытового миксера — энергозатраты снизятся на одну пятую, а качество бетона (или кондитерского крема) улучшится. Лист Мёбиуса используют в велосипедной и волейбольной камере. Совсем недавно ей нашли другое применение - она стала играть роль особенной пружины в заводных игрушках. Такая пружина могла бы стать бесценной – её нельзя перекрутить, как обычную – своего рода вечный двигатель.

Список использованных источников

1. Воронец А.М. Математические развлечения. М.: Учпедгиз, 1981.
2. Гарднер М. Математические досуги. М.: 1992.
3. Кордемский Б.А., Ахадов А.А. Удивительный мир чисел для учащихся. М.: Просвещение, 1996.
4. Кордемский Б.А. Топологические опыты своими руками./ «Квант» №3, 1974,стр73.
5. Коробенок Е.В., Столяр А.А. Сколько сторон у поверхности?: Беседы с учащимися VII-X классов. Минск: Народная асвета, 1995.
6. Леман И. Увлекательная математика. М.: Знание, 1985.
7. Лоповок Л.М. Математика на досуге: Книга для учащихся среднего школьного возраста (IV-VIII классы). М.: Просвещение, 1990.
8. Мубаракзянов Г.М.Математические символы и термины, история их возникновения. Казань: Изд-во “Фән” Академии наук Рт, 2008.
9. Рупасов К.А. Математика на школьной сцене. Тамбов, 1999.
10. Научно-популярный журнал "Квант" 1975год №7, 1977 №7.
11. Интернет – ресурсы:
    http://websib.ru/noos/math/listmebiusa/index.html
    http://canegor.urc.ac.ru/training/2/vozp.htm
    http://host.km.ru/sashka/ho7/lenta.htm

РАЗВИТИЕ 4К–НАВЫКОВ СТУДЕНТОВ ПЕДАГОГИЧЕСКИХ КОЛЛЕДЖЕЙ IT-ТЕХНОЛОГИЯМИ В ПРОЦЕССЕ ОБУЧЕНИЯ

Тафеев Никита Сергеевич, студент 1-го курса
Научный руководитель Губарева Татьяна Викторовна, преподаватель
Автономная некоммерческая профессиональная образовательная организация
«Национальный социально-педагогический колледж», г. Пермь

Одной из приоритетных задач при подготовке специалистов среднего звена, педагогических работников, является создание условий для формирования умений, направленных на саморазвитие и поиск актуальных методов и технологий организации учебной и профессиональной деятельности. Благодаря наличию таких умений, по нашему мнению, выпускник педагогического колледжа не только готов совершенствовать свой уровень подготовки (принцип непрерывности образования), но и способен повышать качество подготовки своих обучающихся.

Модель обучения, согласно которой центральную часть занимают компетенции «4К»: креативность, критическое мышление, коммуникация и кооперация (взаимодействие и сотрудничество) была представлена в докладе «Новый взгляд на образование» на Всемирном экономическом форуме. [1, с.7] Считаем, что принципы «Системы 4К» должны реализовываться и образовательном процессе колледжей, так как провозглашаемые виды базовой грамотности (языковая, числовая, естественно-научная, ИКТ-грамотность, финансовая, гражданско-правовая), компетенции (критическое мышление, креативность, коммуникация и кооперация) и качества характера (любопытство, инициативность, настойчивость, адаптивность, лидерство, социальная и культурная осведомленность), согласно образовательным стандартам [2], находят свое воплощение в требованиях к результатам освоения программы подготовки специалистов среднего звена. Например, общие компетенции, включающие в себя способность:

- «понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;
- организовывать собственную деятельность, определять методы решения профессиональных задач, оценивать их эффективность и качество;
- оценивать риски и принимать решения в нестандартных ситуациях;
- осуществлять поиск, анализ и оценку информации, необходимой для постановки и решения профессиональных задач, профессионального и личностного развития;
- использовать информационно-коммуникационные технологии для совершенствования профессиональной деятельности;
- работать в коллективе и команде, взаимодействовать с руководством, коллегами и социальными партнерами;
- ставить цели, мотивировать деятельность обучающихся, организовывать и контролировать их работу с принятием на себя ответственности за качество образовательного процесса;
- самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации;
- осуществлять профессиональную деятельность в условиях обновления ее целей, содержания, смены технологий».

Так, в соответствии с направлениями реализации «Системы 4К» учитель начальных классов будет обладать 4К-навыками и готов, в рамках своей профессиональной деятельности (преподавание по образовательным программам начального общего образования; организация внеурочной деятельности и общения учащихся; классное руководство; методическое обеспечение образовательного процесса): решать комплексные задачи; думать критически; творчески мыслить; работать в команде; распознавать эмоции других людей и свои собственные, управлять ими; формировать суждения и принимать решения; вести диалог; быстро переключаться с одной задачи на другую.

Данные умения принято называть Soft Skills (гибкие навыки, надпрофессиональные компетенции) в противовес Hard Skills — «жестким» профессиональным навыкам [1]:

- «критическое мышление - это умение ориентироваться в потоках информации, видеть причинно-следственные связи, отсеивать ненужное и делать выводы (чтобы находить решения даже в случае провала, надо понимать причины своих успехов и неудач);

- креативность позволяет оценивать ситуацию с разных сторон, принимать нестандартные решения и чувствовать себя уверенно в меняющихся обстоятельствах;

- коммуникация – ИКТ технологии позволяют находиться на расстоянии телефонного звонка и быть «на связи» 24 часа в сутки. Умение договариваться и налаживать контакты, слушать собеседника и доносить свою точку зрения стало жизненно важным навыком.

- координация (сотрудничество) тесно связана с коммуникацией, но относится к профессиональной сфере. Это умение определить общую цель и способы ее достижения, распределять роли и оценивать результат».

Одним из современных средств освоения теории и практики 4К в образовательном процессе колледжа, по нашему мнению, являются IT-технологии. Именно активное использование IT- технологий в образовательном процессе при интерактивных формах проведения занятий (компьютерных симуляций, деловых и ролевых играх, разбора конкретных ситуаций, психологических и иных тренингов, групповых дискуссий) в сочетании с внеаудиторной работой, прежде всего, способствует качественному формированию и развитию общих и профессиональных компетенций. Широкое применение IT-технологий, объединяющих текст, звук, изображение, способно повысить эффективность активных методов обучения: на этапе самостоятельной подготовки, на лекциях, а также при выполнении заданий практических занятий. Несомненно, самостоятельная работа студента с использованием IT-технологий, при этом, позволяет поставить самостоятельную работу на принципиально новый уровень самостоятельности субъекта обучения.

В настоящее время характерно активное использование возможностей сетевых технологий и дистанционного обучения. Студенты вовлечены в исследовательскую деятельность и уже не являются пассивными слушателями, а сами активно участвуют в подготовке выступлений и различных проектов, выполнении практических заданий и решении профессиональных задач, используя IT-технологии на всех этапах выполнения заданий и решения задач. Таким образом, применение современных IT-технологий обеспечивает новый уровень получения и обобщения знаний студентами, использования их в самостоятельной, проектной и исследовательской деятельности.

При дистанционном обучении и выполнении заданий практических занятий с использованием IT-технологий студенты развивают умения самостоятельно искать, анализировать и отбирать необходимую информацию, организовывать, преобразовывать, сохранять и передавать ее.

Необходимо обратить внимание, что одним из современных средств использования IT-технологий в целях реализации «Системы 4К» для вовлечения студентов в активный процесс обучения и поощрения их критического мышления является web-квест. В общем смысле, web-квест можно определить, как «формат занятия с ориентацией на развитие познавательной, исследовательской деятельности обучающихся, на котором основная часть информации «добывается» через ресурсы Интернета». [1]

Использование интерактивных Интернет-ресурсов в образовательном процессе, таких как: видеоконференции, веб-форумы, дистанционные конференции, социальные сети, несомненно, так же способствуют развитию коммуникативной компетенции студента педагогического колледжа.

Активное включение в образовательный процесс сервисов для создания интерактивных образовательных контентов, содержащих викторины, тесты, дидактические игры и многое другое (например, Kahoot, Quizalize, AhaSlides, Acadly, Wooclap и др.), сервисов для совместной работы по типу бесконечной интерактивной доски для размещения различного контента (например, Google Jamboard, Padlet и др.) направлено не только на

развитие информационной компетентности студентов посредством различных IT-технологий, но и формирование 4К-навыков студентов.

Подводя итог, заметим, - анализ различных источников показал, что технологии обучения «Системы 4К» в настоящее время недостаточно активно используются, однако, существуют общественные проекты, информационно-образовательные сервисы, которые обучают креативности, коммуникации, кооперации и критическому мышлению. Но и образовательные организации, согласно образовательным стандартам, тоже призваны организовать социокультурную среду, создавать условия, необходимые для всестороннего развития и социализации личности, сохранения здоровья обучающихся, способствовать развитию воспитательного компонента образовательного процесса, включая развитие студенческого самоуправления, участие обучающихся в работе творческих коллективов, общественных организаций, что при должной реализации, как раз, способствует достижению целей «Системы 4К». При этом у выпускников педагогических колледжей формируется готовность созданию и проведению уроков нового типа, с активным с использованием различных современных ИКТ.

Список использованных источников

1. Компетенции «4К»: формирование и оценка на уроке: Практические рекомендации / авт.-сост. М. А. Пинская, А. М. Михайлова. — М: Корпорация «Российский учебник», 2019.
2. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 44.02.02 Преподавание в начальных классах (утв. приказом Министерства образования и науки РФ от 27 октября 2014 г. N 1353).
URL: http://ivo.garant.ru/#/document/70809794/paragraph/1:2.

МАТЕМАТИЧЕСКИЙ ПОДХОД К СОЗДАНИЮ САЙТОВ

Штоколов Даниил Романович, студент 2-го курса
Научный руководитель Ткаченко Алла Юрьевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС», Оскольский политехнический колледж, г. Старый Оскол

Математика — это не тоскливые цифры и заученные формулы.
Математика — это логика.
А логика — это творческий подход к решению интересных задач.
Стэнфорда Джо Боулер

Математика – это инструмент, позволяющий человеку осмыслить мир. Это наука о закономерностях. Если взглянуть на мир сквозь призму математики, можно найти ее повсюду: и в океане и дикой природе, архитектуре и осадках, поведении животных и социальных сетях.

Однако для дизайна сайтов и приложений эта наука несправедливо почти не используется. Одним из ключевых показателей качества сайта является визуальное оформление. И если хорошо знать математику, можно использовать ее для интересных, запоминающихся и интригующих конструкций, чтобы пользователю было комфортно пользоваться сайтом.

Золотой прямоугольник

Самому построить не составляет труда: сначала квадрат, затем провести линию от середины одной стороны к противоположному углу и использовать, получившийся отрезок, в качестве радиуса дуги, которая определяет высоту прямоугольника. Последний штрих, достроив секцию, где угол, в который проведен радиус, является правым нижним углом секции, а левый верхний угол ограничен дугой.

Возможное применение

Такую фигуру хорошо использовать для фото-галерей, презентационных сайтов и каталогов продукции. Аккуратный дизайн – шесть золотых прямоугольников**,** по три прямоугольника в каждой строке. Простота изображения создает спокойную атмосферу, и каждый блок акцентирует внимание на своей цели.

Дизайн Фибоначчи

Основан на последовательности чисел Фибоначчи. По определению, два первых числа Фибоначчи равны 0 и 1, и каждое последующее число равно сумме двух предыдущих. Чем больше числа в последовательности Фибоначчи, тем ближе они связаны друг с другом в соответствии с «золотым сечением». Ее можно представить следующим образом: 0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144...

Макет довольно легко построить. Вы выбираете определенную ширину первого блока — например, 90px. Затем, при определении размера контейнера, нужно умножить базовую ширину на номер блока из ряда Фибоначчи (1,2,3,5,8…). В зависимости от расчетов вы получаете значения, которые являются ширинами блоков, для вашего макета.

Возможное применение

Такой дизайн лучше использовать для блогов и журнальных макетов. При этом не следует категорично придерживаться точности цифр, они только опора для творчества.

Пять элементов, или Kundli дизайн

Kundli – это простая фигура, которую может нарисовать каждый. Сначала – квадрат с двумя диагоналями. Смежные середины сторон соединить. У нас получились четыре прямоугольные ромбы. Кстати эту фигуру можно найти в индийских гороскопах.

Возможное применение

Эта фигура, как нельзя лучше подходит для отображения информации о продукте или для показа профилей. Можно украсить шаблон JavaScript анимацией: показать молодые деревца, когда пользователь нажимает на элементе «Земля», или можно показать морское или речное дно, при клике на «Воде».

Синусоидальный дизайн

Всегда есть элемент эксперимента с формулами из физики, химии и других наук или использовать общие формулы.

Рассмотрим синусоидальную волну, или синусоиду. Это математическая функция, которая описывает гладкие повторяющиеся колебания.

Возможное применение

Эта волновая картина часто встречается в природе, включая океанские волны, звуковые или световые. При построении графика среднесуточной температуры. Можно использовать ее, чтобы отображать хронологию событий. Это будет отлично смотреться при горизонтальной навигации.

Вывод. Математика может быть красивой при применении к дизайну. Эти примеры могут помочь в процессе его создания вашего сайта.

Список использованных источников

1. https://theoryandpractice.ru/posts/18531-vo-pervykh-eto-krasivo-prekrasnoe-v-matematike
2. https://habr.com/ru/post/154087/
3. https://multiurok.ru/index.php/files/issliedovatiel-skaia-rabota-po-tiemie-...
4. https://infourok.ru/issledovatelskaya-rabota-po-teme-matematika-v-sozdanii-...

ОСОБЕННОСТИ ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТИ СТУДЕНТА КОЛЛЕДЖА

Яковлева Ксения Геннадьевна, студент 1-го курса
Научный руководитель Губарева Татьяна Викторовна, преподаватель
Автономная некоммерческая профессиональная образовательная организация
«Национальный социально-педагогический колледж» г. Пермь

Исследовательская деятельность - важная часть любого образовательного процесса. На организацию этой деятельности направлены практические занятия, самостоятельные и лабораторные работы, проводятся конкурсы, конференции и другие мероприятия. Ведь, без исследовательской работы не подготовить ни реферат, ни доклад, ни другую подобную работу. Результатом вовлечения студентов в исследовательскую деятельность становится формирование различных профессиональных качеств, например, будущие специалисты, становятся более самоорганизованными, ответственными, учатся отстаивать и формировать позицию, мыслить творчески и неординарно.

Заметим, что сопровождение научным руководителем исследовательской деятельности студентов осуществляется с целью выявить возможности развития активности, креативного потенциала студентов в учебном процессе; формировать интересы, склонности к исследовательской деятельности, умения и навыки проведения исследовательского работы; обучить студентов методике проведения собственных учебных или научных исследований, творчески мыслить и использовать результаты исследования на практике; способствовать профессиональной и социальной адаптации, при это осуществляется поддержка ярких творческих индивидуальностей, способных обеспечить высокий уровень проводимых исследований; доведение результатов исследований и проектов до применения в практической деятельности; ориентация творческих коллективов (групп) на проведение полного цикла исследований и разработок, заканчивающихся созданием готовой продукции; развитие многообразия форм организации научно-исследовательской и творческой деятельности [1].

По нашему мнению, важными направлениями организации самостоятельной исследовательской деятельности студентов является: организация учебной и внеучебной поисково-творческой деятельности; актуализация внутрипредметных и межпредметных связей; изменение характера взаимоотношений «преподаватель – студент – группы обучающихся» в сторону сотрудничества. При этом, исследовательские знания рассматриваются нами, как компонент содержания обучения и включают в себя понимание студентами способов и приёмов работы с информацией, являющихся результатом их познавательной деятельности, направленной на выдвижение, формирование, объяснение закономерностей и фактов, критического отношения. Исследовательские умения - способность осознанно совершать действия по поиску, отбору, переработке, анализу, созданию, проектированию и подготовке результатов исследовательской деятельности, направленной на выявление (создание, открытие) объективных закономерностей фактов или процессов. В ходе овладения исследовательскими знаниями и умениями, по нашему мнению, происходит формирование способности и готовности к выполнению исследовательской деятельности.

Исследовательская работа студентов (обучающихся) может выполняться как индивидуально, так и коллективно. Формы работы определяются в соответствии с уровнем подготовки [2]. В образовательном процессе организация исследовательской работы студентов (обучающихся) осуществляется по двум направлениям:

- теоретическая часть (учебно-исследовательская работа), которая предусматривает изучение студентами методологии исследовательской работы (теоретическая часть), системы закрепления знаний и навыков самостоятельного проведения исследования;
- практическая часть - самостоятельное выполнение практического задания под руководством научного руководителя.

Оба уровня предусматривают элементы исследований как в традиционных формах обучения – практических занятиях, семинарах, лабораторных работах, курсовом и дипломном проектировании, производственной практике, так и работу студентов в научных кружках, инновационных работах, участие студентов в международных исследованиях, в конкурсах на получение грантов.

Отметим, что участие в исследовательской работе помогает студентам постигать специфику своей специальности, применять знания в решении практических задач, развивает навыки работы в коллективе. Так, в процессе выполнения учебных исследований студенты учатся пользоваться приборами, оборудованием, самостоятельно проводить эксперименты, применять свои знания при решении конкретных задач исследовательского характера.

Механизм исследовательского обучения в кратком виде может быть выражен такой последовательностью: преподаватель ставит перед студентами проблему (либо подводит студентов к формулированию проблемы) и показывает на ее примере образец организации и проведения исследования. Это предполагает, что студент: выделяет и ставит проблему; предлагает возможные решения; делает выводы в соответствии с результатами проверки; применяет выводы к новым данным; делает обобщения. Таким образом, развиваются умения [3]:

- планирования (составление плана, выстраивание логики содержания, постановка цели, реализация цели);
- наблюдения (оценка достигнутого, ответы на вопросы для самоконтроля, применение теории на практике, составление тезисов по теме, обращение к разным источникам);
- регуляции (самооценка, использование дополнительных ресурсов, волевая регуляция, определенная последовательность выполнения задания).

Особенностью организации такой деятельности студентов является следующее [2]:

- учебные проблемы отвечают личным и профессиональным потребностям студентов;
- ведущая роль педагога сохраняется, но у студентов сохраняется ощущение, что проблема и способы ее решения выбраны ими самостоятельно;
- избираемые студентами темы, обычно, выходят за рамки одной дисциплины.

Приведем примеры основных форм представления исследовательской работы студентов: доклад; сообщение по теме; дневник наблюдений; алгоритм решения конкретной задачи; аннотированный библиографический список; терминологический словарь; реферат; аннотация; план решения проблемы (педагогической или иной производственной задачи).

Таким образом, самостоятельная работа студентов направлена на совокупность аудиторных и внеаудиторных занятий и работ, обеспечивающих успешное освоение образовательной программы. Заметим, что к началу обучения в колледже студент уже имеет личный опыт и навыки организации собственных действий, полученные в процессе обучения в школе, учреждениях дополнительного образования, во время внешкольных занятий и в быту. Однако, при обучении в колледже требования к организации самостоятельной работы возрастают, так как они связаны с освоением профессиональных компетенций.

Таким образом, самостоятельная исследовательская деятельность студента колледжа призвана решать следующие задачи: закрепление и расширение знаний, умений по дисциплинам учебного плана, приобретение дополнительных знаний и навыков, в том числе развитие навыков, связанных с исследовательской деятельностью; развитие навыков самоорганизации и формирование самостоятельности мышления, способности к саморазвитию, самосовершенствованию и самореализации.

Список использованных источников

1. Федеральный государственный образовательный стандарт среднего профессионального образования по специальности 46.02.01 Документационное обеспечение управления и архивоведение (утв. приказом Министерства образования и науки РФ от 11 августа 2014 г. N 975). URL: http://ivo.garant.ru/#/document/70730762/paragraph/1.

2. Куликова Т.А. Активизация познавательной деятельности студентов при работе в онлайн-формате. - Материалы научной конференции научно-педагогических работников, аспирантов, магистрантов: УНИВЕРСИТЕТ XXI ВЕКА: НАУЧНОЕ ИЗМЕРЕНИЕ. - ТГПУ им. Л. Н. Толстого. - Тула, - 2020. - С. 35.

3. Губарева Т.В. О проблеме определения показателей информационной компетентности студентов. - Научно-методический электронный журнал «Концепт». - 2015. - № Т30. - С. 73.

Секция 1.6

АНАЛИЗ ВЛИЯНИЯ ПАНДЕМИИ КОРОНАВИРУСА НА МАЛЫЙ БИЗНЕС В РОССИЙСКОЙ ФЕДЕРАЦИИ

Арская Алина Сергеевна, студент 2 курса
Кувашова Людмила Владимировна, студент 3 курса
Научный руководитель Пихтерева Марина Алексеевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Исследованиями последствий пандемии covid – 19 ученые всего мира будут заниматься еще очень и очень долго. До конца не изучен сам вирус, появляются новые штаммы, за второй волной следует третья. Сам вирус и ограничительные меры, связанные с ним, оказали колоссальное влияние на жизнь людей во всем мире.

Наша работа посвящена, пожалуй, одному из самых пострадавших объектов экономики – малому предпринимательству. Последнее представляет собой один из важнейших секторов экономики, способствующих развитию конкурентной рыночной среды, наполнению потребительского рынка товарами и услугами, созданию новых рабочих мест, формированию широкого круга собственников, развитию малых форм производства, что свидетельствует об актуальности проблемы исследования.

Если говорить более конкретно, то нас интересовало, насколько сильным оказалось влияние пандемии на малый бизнес в нашей стране.

Принято считать, что история малого бизнеса в России (тогда еще в СССР) начинается в 1987 – 1988 гг., когда эта сфера деятельности начала расширяться, количество людей, принимающих в нем участие, увеличиваться, предпринимательство стало приобретать характер активного многочисленного движения [1].

Что же касается современной истории, то сегодня в экономической науке не существует единого подхода к определению «малого предпринимательства» [4]. А в отечественной литературе и вовсе данное понятие одновременно отождествляют с: сектором экономики, экономической категорией и хозяйственной системой [4].

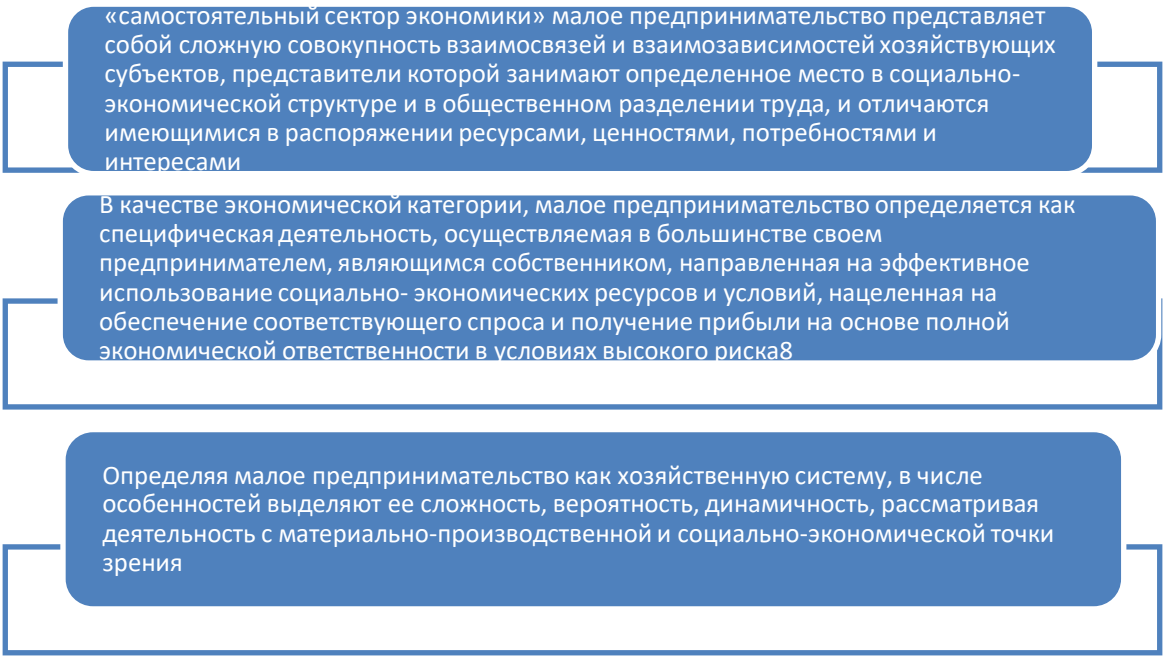


Рис. 1 – Подходы к определению «малое предпринимательство»

В действующем российском законодательстве конкретное определение малого предпринимательства не сформулировано, однако говорится о том, что это хозяйствующие субъекты, к которым относят юридических лиц и индивидуальных предпринимателей, отвечающих ряду критериев, закрепленным в нормах Федерального закона «О развитии малого и среднего предпринимательства».

В работе также говорится о проблемах, которые существовали в среде малого предпринимательства до пандемии. По мнению, самих предпринимателей (опрос 2019 г от Альфа-банка) главные проблемы выглядят следующим образом [2]: снижение покупательского спроса, высокие налоги, недостаток кадров.

Если же говорить о мнении экспертного сообщества, то здесь отмечается острая конкуренция, несовершенство налоговой и законодательной базы, сложности кредитования, региональный аспект, административное давление.

На наш взгляд, пандемия covid – 19 лишь обнажила указанные проблемы, сделав их еще более острыми.

По данным апрельского замера Индекса RSBI – ежемесячного исследования бизнес-настроений малого и среднего бизнеса, организованного «Промсвязьбанком» (ПСБ) совместно с «Опорой России», после введения режима самоизоляции падение спроса отметили 80% предпринимателей сектора малого и среднего бизнеса [5]. То есть проблема спроса действительно стала еще насущнее.

В разрезе по размеру бизнеса наиболее пострадали микропредприятия – среди них падение спроса отметили 85% опрошенных. Малый и средний бизнес пострадал немного меньше: спрос упал у 74% и 76% соответственно[7].

Что касается видов деятельности, то здесь ожидаемо сильнее всех пострадали сферы услуг и торговли – сокращение спроса зафиксировали 82% и 81% предпринимателей соответственно. Промышленные предприятия отметили меньшее падение, спрос сократился у 73%[6,7].

Наконец, согласно первой оценке Росстата, ВВП страны упал по итогам 2020 года на 3,1%, а реальные доходы граждан уменьшились на 3,5%, безработица достигла 5,9 %. [3].

«Согласно исследованиям и статистике, прекратило работу 1,95 млн малых и средних предприятий, это почти каждый пятый в России. Общее число МСП сократилось более чем на 240 тыс., или на 4,2%, до 5,6 млн.», - сообщил член генерального совета «Деловой России» Алексей Мостовщиков [3].

Отметим также меры поддержки малого и среднего бизнеса в нашей стране государством в период пандемии [6]:

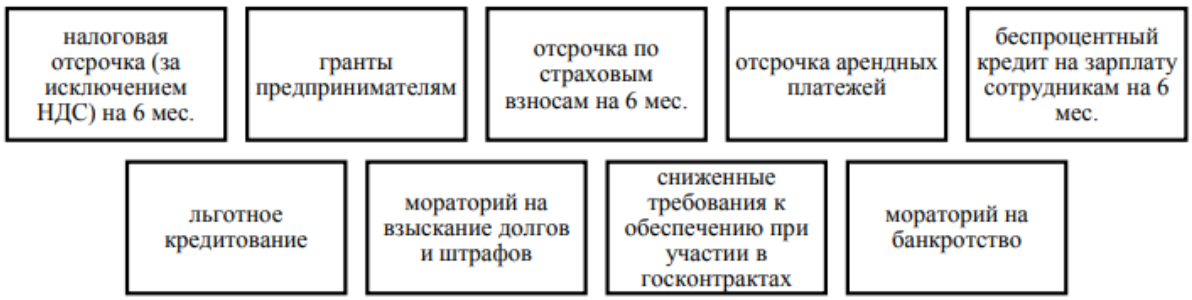


Рис. 2 – Меры поддержки малого и среднего бизнеса в РФ в период пандемии

Здесь стоит добавить, что к концу 2020 указанные мероприятия несколько смягчили удар коронавируса по малому бизнесу.

Так, по данным контрольно-кассовой техники, обороты по сектору МСП за полтора месяца 2021 года на 90% восстановились до уровня начала 2020 года [3].

Учитывая колоссальное падение спроса, падение реальных доходов граждан, рост безработицы, серьезные ограничительные меры с одной стороны, и помощь со стороны

государства как для малых предприятий, так и для граждан, а также постепенный рост спроса к марту 2021 года, в заключении исследования делаются следующие выводы:

- нельзя забывать о пандемии, то есть ведение бизнеса должно быть с оглядкой на рекомендации властей, необходим постоянный мониторинг ситуации, знание, в данном случае, действительно сила;

- со стороны государства, на наш взгляд, требуется дополнительное стимулирование спроса населения, а также продолжение оказания поддержки малому бизнесу, поскольку эти два элемента тесно взаимосвязаны.

В заключении, на наш взгляд, можно сказать, что помимо целого ряда отрицательных моментов, пандемия в итоге приведет к снижению числа конкурентов на рынке (то есть останутся самые сильные и умелые), к появлению новых видов трудовой деятельности (например, дистанционный режим работы в прежние времена не пользовался популярностью), к накоплению опыта ведения бизнеса в подобных «шоковых условиях».

Таким образом, влияние covid – 19 нельзя охарактеризовать однозначно «кошмарным» для малого бизнеса в нашей стране, хотя негативных моментов действительно больше, однако после кризиса всегда идет подъем, надеемся, что он уже начался.

Список использованных источников

1. Батуро А.Ю. Проблемы и перспективы развития малого бизнеса в России// Научно – методический электронный журнал «Концепт». – 2017. – Т.39. – С.281 – 285

2. Волкова О., Малый бизнес назвал четыре главные проблемы. – [Электронный ресурс] - Режим доступа: https://www.top.rbc.ru/economics/25/09/ 2015/

3.Доклад «Социально-экономическое положение России» – [Электронный ресурс]. – Режим доступа: https://rosstat.gov.ru/compendium/document/50801

4. Кремин А.Е. Теоретические подходы к определению категории малого предпринимательства //Экономика и социум. - 2015. - № 3-1 (16). - С. 959-967

5. Осведомлен – значит вооружен. Как будет развиваться нынешний кризис // [Электронный ресурс]. – Режим доступа: https://quote.rbc.ru/news/article /5e9464be9a7947a7d1a39918?utm_refen.yandex.com

6. Парламент принял новый пакет законов для поддержки граждан в условиях коронавируса. – [Электронный ресурс]. – Режим доступа: http://duma.gov.ru/news/48320/

7. 80% компаний МСП отметили снижение спроса с начала пандемии коронавируса – [Электронный ресурс]. – Режим доступа: https://www.psbank.ru/Bank/Press/News/2020/06/01-01

ОСОБЕННОСТИ ИНФЛЯЦИИ В РОССИИ

Бабкина Дарья Сергеевна, студент 2-го курса
Научный руководитель Богданова Екатерина Николаевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Инфляция — это переполнение каналов денежного обращения избыточной денежной массой, проявляемое в росте товарных цен.

Сам термин «инфляция» возник в связи с массовым переходом национальных денежных систем к обращению неразменных бумажных денег. Первоначально в экономический смысл инфляции был вложен феномен избыточности бумажных денеги в связи с этим их обесценение.

Сущность инфляции экономисты трактуют по-разному:

- переполнение каналов денежного обращения избыточными бумажными деньгами, вызывающими их обесценивание по отношению к золоту, товарам, иностранной валюте, сохраняющей прежнюю реальную ценность или обесценившейся в меньшей степени;
- как любое обесценивание бумажных денег;
- как повышение общего уровня цен;
- как многофакторный процесс, не имеющий однозначного толкования

Инфляция проявляется в различных формах, основными из которых являются:

1) рост цен на товары и услуги, причем неравномерный, что приводит к обесцениванию денег, снижению покупательской способности;

2) понижение курса национальной денежной единицы по отношению к иностранной. Например, в 1991г. доллар США равнялся 90 коп., а на 2011г. 1 доллар США равен 29 руб. 39 коп.

3) увеличение цены драгоценных металлов (серебро, золото, палладий, платина и т.д.).

Главные причины инфляции - это:

1. Отсутствие баланса между госрасходами и госдоходами. Появляющийся дефицит бюджета закрывается при помощи запуска печати новых дензнаков, что ведет к росту объема денежной массы и к инфляции.

2. Недостаток пространства для рыночных отношений и отсутствие нормальной конкуренции.

3. Ввозимая инфляция импорта, этот фактор влияет все больше и больше, так как в связи с процессом глобализации экономики стран становятся более открытыми.

4. Ожидания инфляции. Люди постоянно думают о повышении цен, ждут их, поэтому стараются запастись необходимым, а продавцы в свою очередь в цену продукции стараются заложить возможный рост издержек.

В каждой стране инфляционный процесс имеет специфику, связанную с совокупностью причин и факторов, его вызывающих.

Современную инфляцию в России нельзя рассматривать без учета специфики планово-распределительной системы хозяйствования, без учета политических и экономических процессов, произошедших за последние годы.

Важным фактором инфляционных процессов в стране выступала планово-распределительная система хозяйствования. Она породила затратный механизм хозяйствования и нарушение материальной и денежной сбалансированности в народном хозяйстве, что объяснялось диспропорциями во всех сферах экономики, прежде всего:

· в распределении национального продукта на фонд накопления и фонд потребления и на базе этого проведении активной инвестиционной политики;

· в производстве средств производства и товаров народного потребления;

· в системе государственного ценообразования;
· доходах и расходах государственного бюджета (дефицит);
· в кредитных и финансовых ресурсах.

Зарождавшиеся инфляционные процессы в нашей стране были обусловлены диспропорциями в сложившейся структуре народного хозяйства, в которой предпочтение отдавалось производству средств производства и вооружений при недостаточном уровне промышленного производства потребительских товаров и услуг, слабом развитии сельского хозяйства при огромных и неэффективных инвестициях в него.

Огромной проблемой для экономики России при регулировании инфляционных процессов становятся внешние займы. Не решив ни одной экономической, социальной и политической проблемы с помощью иностранных кредитов, их активно использовали для покрытия бюджетного дефицита, который из года в год нарастал и требовал еще больших заимствований.

Важнейшим фактором нарастания инфляции в России явилась дальнейшая либерализация валютного законодательства, внешней торговли, устранение валютных ограничений по текущим операциям, введение внутренней конвертируемости рубля в условиях огромной внешней задолженности государства.

Таблица инфляции за последние 3 года: данные Росстата и ЦБ РФ

Каждое число в таблице указывает на размер инфляции за месяц.

Год	Янв.	Фев.	Мар.	Апр.	Май	Июнь	Июль	Авг.	Сен.	Окт.	Ноя.	Дек.	Всего
2021	1.462	0.67	0.78	-	-	-	-	-	-	-	-	-	-
2020	4.91	0.40	0.33	0.55	0.83	0.27	0.22	0.35	-0.04	-0.07	0.43	0.71	0.83
2019	3.05	1.01	0.44	0.32	0.29	0.34	0.04	0.20	-0.24	-0.16	0.13	0.28	0.36
2018	4.27	0.31	0.21	0.29	0.38	0.38	0.49	0.27	0.01	0.16	0.35	0.50	0.84

В 2018 году уровень инфляции в России составил 4,27%, что на 1,75 больше, чем в предшествующем 2017 году и на 1,22% больше, чем в следующем 2019.

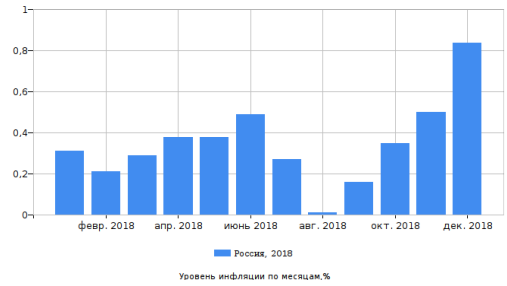


Рисунок 1- Уровень инфляции 2018г

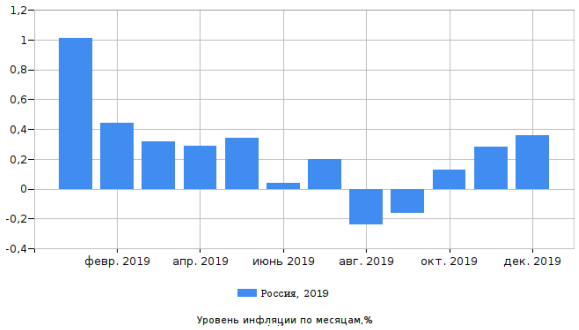


Рисунок 2- Уровень инфляции 2019г

В 2019 году уровень инфляции в России составил 3,05%, что на 1,22 меньше, чем в предшествующем 2018 году и на 1,87% меньше, чем в следующем 2020.

В 2020 году уровень инфляции в России составил 4,91%, что на 1,86 больше, чем в предшествующем 2019 году.

Постараемся обобщить причины, влияющие на проявления инфляции в России. К таким причинам можно отнести:

- во-первых, несбалансированность государственных расходов и доходов, выражающаяся в дефиците госбюджета. Если этот дефицит финансируется за счет займов в Центральном эмиссионном банке страны, другими словами, за счет активного использования «печатного станка», это приводит к росту массы денег в обращении.

- во-вторых, инфляционный рост цен может происходить, если финансирование инвестиций осуществляется аналогичными методами. Особенно инфляционно опасными являются инвестиции, связанные с милитаризацией экономики. Так, непроизводительное потребление национального дохода на военные цели означает не только потерю общественного богатства. Одновременно военные ассигнования создают дополнительный платежеспособный спрос, что ведет к росту денежной массы без соответствующего товарного покрытия. Рост военных расходов является одной из главных причин хронических дефицитов государственного бюджета и увеличения государственного долга во многих странах, для покрытия которого государство увеличивает денежную массу.

- в-третьих, общее повышение уровня цен связывается различными школами в современной экономической теории и с изменением структуры рынка в XX веке. Современный рынок — это в значительной степени олигополистический рынок. А олигополист обладает известной степенью власти над ценой. И если даже олигополии не первыми начинают «гонку цен», они заинтересованы в ее поддержании и усилении.

- в-четвертых, с ростом «открытости» экономики той или иной страны, все большим втягиванием ее в мирохозяйственные связи увеличивается опасность «импортируемой» инфляции через рост цен на импортное сырье, через потоки спекулятивных капиталов и т. д.

- в-пятых, инфляция приобретает самоподдерживающийся характер в результате инфляционных ожиданий. Инфляция может воспроизводиться и из-за политической нестабильности.

Рисунок 3 – Прогрессивный уровень инфляции в 2020г

Антиинфляционная политика – комплекс мер, разработанных государством, по предотвращению или сдерживанию возникшей инфляции.

Инфляция является неотъемлемой частью рыночной системы хозяйствования. В мире накоплен богатый опыт форм и методов антиинфляционной политики. Целью этой политики является создание таких условий функционирования рыночной системы, при которых инфляция была бы управляема, а ее уровень – умеренным.

Обычно выделяют два основных направления антиинфляционной политики государства: *адаптивную политику*, предполагающую приспособление к инфляции, смягчение ее последствий, и *активную политику*, направленную на ликвидацию причин инфляции.

Суть адаптивной политики сводится к тому, что правительство с определенной периодичностью индексирует основные виды фиксированных доходов населения (минимальная заработная плата, пенсии, стипендии и т.п.). Обычно индексация составляет 60—70 % от уровня инфляции. Делается это для того, чтобы, с одной стороны, поддерживать минимально достаточный уровень доходов населения, а с другой стороны, за счет разницы в 30—40 % постепенно, за полтора-два года, снизить спрос на национальном рынке и тем самым погасить инфляцию. Этот метод борьбы с инфляцией имеет как достоинства, так и недостатки. Явное его преимущество — социальная стабильность в обществе. В качестве недостатка можно упомянуть длительность сроков реализации данного подхода к борьбе с инфляционными явлениями.

Активная политика борьбы с инфляцией осуществляется на основе значительного сокращения количества денег, находящихся в обращении. Это предполагает, проведение денежной реформы конфискационного типа; контроль за денежной эмиссией; недопущение эмиссионного финансирования государственного бюджета; текущий контроль за состоянием денежной массы в рамках осуществления кредитно-денежной политики. Реализация политики активной борьбы с инфляцией позволяет свести инфляцию почти к нулю за достаточно короткий промежуток времени.

Изложенное в даннойстатье позволяет сделать следующие выводы:

1. В настоящее время инфляция - один из самых болезненных и опасных процессов, негативно воздействующих на финансы, денежную и экономическую систему в целом. Инфляция означает не только снижение покупательной способности денег, она подрывает возможности хозяйственного регулирования, сводит на нет усилия по проведению структурных преобразований, восстановлению нарушенных пропорций.
2. К негативным последствиям инфляционных процессов относятся снижение реальных доходов населения, обесценение сбережений населения, потеря у производителей заинтересованности в создании качественных товаров, ограничение продажи сельскохозяйственных продуктов в городе деревенскими производителями в силу падения заинтересованности, в ожидании повышения цен на продовольствие, ухудшение условий жизни преимущественно у представителей социальных групп с твердыми доходами (пенсионеров, служащих, студентов, доходы которых формируются за счет госбюджета).
3. Нормализация денежного обращения и противодействие инфляции требуют выверенных, гибких решений, настойчиво и целеустремленно проводимых в жизнь.

Список использованных источников

1. Центральный банк Российской Федерации Банк России Официальный сайт https://cbr.ru
2. Федеральная служба государственной статистики Официальный сайт https://rosstat.gov.ru
3. Финансы : учебник и практикум для среднего профессионального образования / Л. А. Чалдаева [и др.] ; под редакцией Л. А. Чалдаевой. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2021. — 491 с. — (Профессиональное образование). — ISBN 978-5-534-14782-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/481863 (дата обращения: 07.04.2021).
4. Финансовая экономика - журнал ВАК по экономике и правуhttps://finanec.ru

«ЧЕЛОВЕК, КОТОРЫЙ ВЕСЬ БОРЬБА»

Башкатова Дарья Алексеевна, студент 1 курса
Научный руководитель Левченко Татьяна Николаевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

2021 год в России Указом Президента страны В.В. Путина объявлен годом Достоевского. Отмечается сразу несколько знаменательных дат, связанных с именем писателя – 515 лет роду Достоевских, 140 лет со дня его смерти, и юбилейная дата - 200 лет со дня рождения Федора Михайловича. Весь 2021-й год пройдет под эгидой празднования этого знакового юбилея.

В рамках юбилейных мероприятий создан электронный портал «Мир Достоевского», по всей стране проводятся массовые чтения, квесты, театральные постановки, экскурсии.

Поэтому тема нашей работы актуальна.

«Человек, который весь борьба». Так сказал о Достоевском Лев Николаевич Толстой. Преодоление себя, поиски истины, переживания и ошибки — все это Федор Михайлович испытал в полной мере.

Исследовав художественные тексты, научно – критическую литературу, монографии по теме исследования, мы попытались понять, чему же Достоевский учит нас, что может дать нам, современным людям, писатель, живший в 19 веке. Быть может мысли и выводы, к которым он приходит, сегодня неактуальны? Почему он остаётся одним из самых читаемых писателей в мире?

Чтобы чувствовать себя человеком в мире людей, мы должны задать себе вопросы: для чего и как мы живем? Что может себе человек? Где границы человеческой свободы? Великий писатель событиями своей жизни, через свой взгляд на мир, на человека, указывает нам путь к самим себе. И мы начинаем слышать собственную душу. В первую очередь нужно попытаться разгадать себя, найти в себе самом человека.

Достоевского еще при жизни одни считали гением, почти святым, другие называли сумасшедшим. Он все время находился на грани, на краю. Не миновал ни тюрьмы, ни сумы. Стоял на эшафоте, глядя в лицо смерти, убивал себя азартной страстью в казино, отдавал последние деньги нечестным кредиторам брата, снова возрождался для жизни и творчества,
Федор Михайлович Достоевский родился в семье военного врача, жившего в Москве. «Русский бунт, беспощадный», от которого предостерегал Россию А.С. Пушкин, не миновал семью Достоевских. Отец Федора Михайловича, Михаил Андреевич, по воспоминаниям родственников и устным преданиям, был убит своими крестьянами.

С января 1838 Достоевский учится в Главном инженерном училище. Как мы знаем теперь, инженерное училище расположено в замке, в котором был убит, с молчаливого согласия сына, будущего императора Александра I, император Павел I. Позднее нравственная схема отцеубийства сработает в романе Достоевского «Братья Карамазовы». Что это: случайное совпадение или умение вглядываться в невидимую, тайную суть вещей, обладание особой прозорливостью?

В 1845 году после многочисленных переделок Достоевский заканчивает роман «Бедные люди». Произведение имело исключительный успех. Литературный критик Белинский написал: *«Честь и слава молодому поэту, муза которого любит на чердаках и в подвалах и говорит о них обитателям раззолоченных палат: «Ведь это тоже люди, ваши братья!»* В «Бедных людях» в полной мере проявилась особенность творческого метода Достоевского, о которой он сам сказал: **«Меня зовут психологом - неправда, я лишь реалист в высшем смысле, т.е. изображаю все глубины души человеческой».** *Роман*

«Бедные люди» - вздох сожаления по всему человечеству. **Это эпиграф ко всей будущей прозе Достоевского.**

С марта - апреля 1847-го года Достоевский участвует в организации тайной типографии для печатания воззваний к крестьянам и солдатам. Фёдор Михайлович разделяет идею отмены крепостного права и цензуры в литературе. Но в отличие от остальных петрашевцев, является противником насильственного свержения существующей власти. Достоевский прекрасно понимает, что заговор обречен, но сам, добровольно меняет свою судьбу, наверное, это ***акт самопознания***.

23 апреля 1849 года он вместе с другими петрашевцами был арестован и заключен в Алексеевский равелин Петропавловской крепости. Они были приговорены к смертной казни. На середине площади был сооружен деревянный эшафот со ступенями и врытыми в землю столбами. С осужденных сняли верхнюю одежду, и они стояли на двадцатиградусном морозе в одних рубашках. Казнь уже началась. Но в тот момент, когда, должна была раздаться команда «пли», один из высших военных чинов взмахнул белым платком. Был объявлен новый приговор. Достоевскому назначалась каторга на четыре года, и потом служба рядовым в Сибири. Достоевский до каторги и после нее – совершенно разные люди.

Достоевский был счастлив в семейной жизни. Это счастье подарила ему вторая жена, Анна Григорьевна Сниткина. Женщина, ради которой он сумел справиться с пагубной страстью – тягой к рулетке. Однажды пообещав ей не играть, Достоевский больше не подходит к казино. Достоевского спасла любовь, так как только в любовном согласии люди могут победить в себе злые влечения.

Умер Федор Михайлович 28 января 1881 года. Похоронен в Александро-Невской лавре в Петербурге.

Мало известна деятельность Достоевского – публициста. Он издает журналы «Время» и «Эпоха», принимает на себя редакторство журнала «Гражданин». *Впервые в России выпускается «моножурнал»,* т.е. Достоевский единолично является его и редактором, и автором. В "Гражданине" Достоевский осуществляет давно задуманную им идею "Дневника писателя", публикует ряд статей и заметок. *Впервые в России писатель лично получает огромное количество писем,* впервые устанавливаются взаимоотношения между читателем и писателем.

Внимание писателя привлекают железнодорожные катастрофы, судебные процессы, распространение самоубийств среди молодежи. Его беспокоит распад семейных связей, эпидемия пьянства, искажение русского языка и многие другие «больные» вопросы.
«Дневник писателя» - страстный призыв к самосовершенствованию человека, к напряженному труду над собой.

Имя Достоевского связано и с нашим родным краем, Белгородчиной. Первый биограф Достоевского, литературный критик, философ, публицист Н.Н. Страхов родился в Белгороде. **Ф.М. Достоевский был замечательным педагогом**. Им разработана целая система воспитания детей. Гуманизм Ф.М. Достоевского проявляется в первую очередь к тем, кто не может постоять за себя: маленьким детям. Гуманизм по Достоевскому - это сострадание, жалость к ближнему.

Его принципом было не подтягивать детей на свой взрослый уровень, а понимать ребенка. Ф.М. Достоевский никогда в своих работах не использовал слово «воспитывать», а употреблял совершенно другие слова – «наблюдай», «веди».

Самое главное в творчестве Достоевского – это воспитание души. Достоевский держит читателя в постоянном напряжении, вынуждает его спрашивать себя: «А нет ли в твоей душе стремления к душевной лени? Не слабеет ли в самом себе голос совести? Нет ли в тебе жестокости? Жива ли в тебе человеческая душа?»

Чтобы понять, актуально ли творчество Достоевского, нужно ли оно современной молодежи, было проведено практическое исследование среди студентов 1 курса Оскольского политехнического колледжа в количестве 54 человек. Результаты таковы: 77% опрошенных знакомы с произведениями Достоевского поверхностно, 23% - читали произведения. 81%

респондентов считают творчество писателя актуальным, 79% согласились с мнением Достоевского, что каждый человек лично ответственен за царящее в мире зло. Однако 14% отметили, что они не готовы нести ответственность за свои поступки, и 3% ответили, что не готовы отказаться от вредных привычек ради близкого человека.

Большинство студентов ответили, что творчество Достоевского помогает им в выработке нравственного характера, духовной мужественности. Величие писателя в том, что он показал нам, как во тьме возгорается свет, и что этот свет есть в каждом человеке.

Современный человек живет в тех же условиях, что и герои Достоевского. Современная кризисная ситуация в России и в мире в целом (обострение национальных и социальных отношений, духовный кризис человечества) в известной мере была предсказана Достоевским в его художественно-философских исследованиях. Социально-философские открытия писателя, таким образом, могут быть *востребованы современной молодежью для предотвращения социальной и духовной катастрофы.*

При создании романа «Братья Карамазовы» Ф.М.Достоевский выделит в эпиграф слова из Евангелие: «Истинно, истинно глаголю вам: аще пшеничное зерно, падши в землю, не умрет, то останется одно; а если умрет, то принесет много плода». Сам Достоевский – это и есть *то зерно,* он умирает (переживает момент смерти, стоя на эшафоте), но перерождается, дает много плодов, чтобы все последующие поколения могли вкусить их и задуматься о цели и смысле своей жизни, смогли лучше понять себя, научились сострадать и любить ближнего своего.

По словам Н.А. Бердяева, Достоевский и «есть та величайшая ценность, которой оправдает русский народ свое бытие в мире, то, на что может указать он на Страшном Суде народов».

Список использованных источников

1. Абельтин, Э.А. Актуальность творчества Ф.М. Достоевского. 1999.URL: http://www.neuch.ru/referat/89366.html(дата обращения 16.03.2021)
2. Бахтин, М.М. Проблемы поэтики Достоевского / М.: «Художественная литература», - 1972. – 471с.
3. Бердяев, Н.А. Откровение о человеке в творчестве Достоевского. 2011. URL: /http://www.repetitor.org/materials/dostoevsky2.html(дата обращения 12.10.2020)
4. Достоевский как редактор и издатель. 1996. URL: http://www.petaref.com/?page=viewref&id=9330(дата обращения 07.10.2020)
5. Степанов, А.В. Дискурсы Ф.М. Достоевского // Русский язык в школе. - 2006г. – №5 - 67с.
6. Ф. М. Достоевский: жизнь и творчество. 2017.URL: http://www.rsl.ru /ru/s3/s331/s122/d306/ (дата обращения 17.03.2021)
7. Электронная библиотека – Википедия// URL:https://ru.wikipedia.org /wiki/Достоевский,_Фёдор_Михайлович (дата обращения 27.03.2021)

ИСПОЛЬЗОВАНИЕ ДИАГРАММЫ ГАНТА И МОДЕЛИ ОСТЕРВАЛЬДЕРА ПРИ ПЛАНИРОВАНИИ РАБОЧЕГО ПРОЦЕССА

Кувашова Людмила Викторовна, студент 3-го курса
Научный руководитель Василевская Галина Николаевна, преподаватель
Старооскольский технологический институт им. А.А.Угарова (филиал) Федерального государственного автономного образовательного учреждения высшего образования "Национальный исследовательский технологический университет "МИСиС", Оскольский политехнический колледж, г. Старый Оскол

При планировании рабочего процесса, необходимо пройти определенные цикл этапов реализации бизнес - идеи. Для регистрации организации необходимо: принять решение на создание ООО или ИП; выбрать тип налогообложения; сформировать Устав если открывается ООО; оплатить госпошлину; подать документы в ФНС, при этом получить расписку с перечнем всех поданных документов; получить документы в налоговой инспекции, после этого она должна зарегистрировать юридическое лицо и внести его в государственный реестр в течение пяти дней; заказать печать; открыть расчетный счет в банке; обратиться во внебюджетные фонды для присвоения кодов статистики и лицевых счетов; заключить договор аренды; подписать договоры с поставщиками; подобрать специалистов и обслуживающий персонал; приобрести оборудование. Следующий этап - это разрешительные документы.

Рисунок 1- Диаграмма Ганта

Наглядно все этапы процесса планирования рекомендуется размещать в диаграмме Ганта, используя Excel. Модель А. Остервальдера помогает системно походить к планированию. Например:

Таблица 1- Модель Остервальдера

<table>
<tr><td rowspan="2">Ключевые партнёры
Оптовики;
Аутсорсинг;
другие розничные магазины.</td><td>Виды деятельности
Производство и продажа</td><td rowspan="2">Ценностные предложения
Цена ниже чем у конкурентов;
предзаказ по каталогу через интернет.</td><td>Отношения с покупателями
Проведение рекламных акций</td><td rowspan="2">Сегментация потребностей
Низкий ценовой сегмент; средний ценовой сегмент; высокий ценовой сегмент; премиум.</td></tr>
<tr><td>Ключевые ресурсы
Аренда помещения</td><td>Каналы взаимодействия
Группы в социальных сетях;
Свой сайт.</td></tr>
<tr><td colspan="3">Структура затрат
Закупка товара;
Зарплата продавцов;
Аренда помещения;
Налоги и сборы;
Коммунальные услуги.</td><td colspan="2">Поток поступления доходов
Торговая выручка в магазине;
Выручка от онлайн – продаж.</td></tr>
</table>

Швейцарский ученый и бизнесмен Александр Остервальдер и его коллега Ив Пинье разработали универсальную методику, с помощью которой можно создать или проверить уже существующую бизнес-модель для любой сферы деятельности. Основа любого бизнеса - это клиенты. Если товары или услуги не будут покупать, говорить о создании и развитии компании бессмысленно.

На этом этапе необходимо определить, кого может заинтересовать ваш продукт - выделить для себя целевую аудиторию. Далее сегментирование будущих клиентов – их необходимо разделить на группы: по возрасту, уровню дохода, семейному положению, предпочтениям. Чем подробнее это сделано, тем проще будет в дальнейшем составлять модель и строить бизнес.

В итоге должны получиться конкретные портреты потенциальных клиентов.

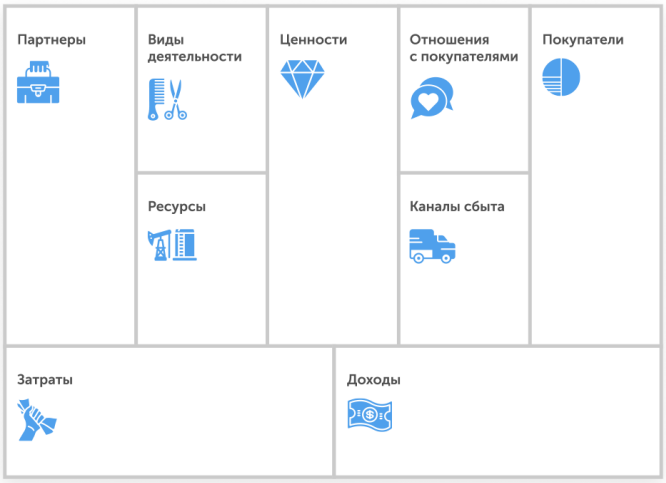


Рисунок 2 – Рекомендуемая таблица для модели Остервальдера

Список использованных источников

1. Анискин Ю.П. Управление инвестициями: учеб. пос. для вузов. - 3 - е изд., стер. - М.: Омега - Л, 2019. - 192 с.

2. Михайлов А.А. Основные правила создания своего дела для начинающих предпринимателей - М: Просвещение, 2020.- 170 с.

3. Рыжих О.Н. «Легко ли быть предпринимателем?»- М.: Дрофа,2019.- 302 с.

4.Халтаева С.Р. Яковлева И.А. Бизнес – планирование: Учебное пособие – Улан – Удэ, 2018 . – 574 с.

ОСОБЕННОСТИ ПОЛИТИКИ ЖИЛИЩНОГО СТРОИТЕЛЬСТВА В СССР В 1960-70-Е ГГ.

Панкратова Елизавета Николаевна, студент 1 курса
Научный руководитель Слободенюк Наталия Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Противоречивая советская эпоха ушла в прошлое. Но до сих пор данный этап отечественной истории вызывает много споров, неоднозначных оценок. Кто-то испытывает ностальгию, вспоминая пионерское детство и комсомольскую юность. Находятся и критики, указывающие на имевшиеся проблемы и упущенные возможности. Такая же разноплановая характеристика даётся десятилетию правления Н.С. Хрущёва и, в частности, его программе обеспечения населения жильём, которая реализовывалась в СССР с середины 1950-х гг.

Данное исследование – это попытка проанализировать все достоинства и недостатки политики жилищного строительства, выявить её особенности и конечные результаты. В связи с тем, что так называемые «хрущёвки» остаются в составе жилищного фонда многих населённых пунктов России до сих пор, данная тема представляется нам актуальной.

Послевоенное восстановление и стремительная индустриализация СССР в 50-е годы XX века привели к тому, что сельское население начало массово переезжать в крупные города. Свободных жилых помещений было мало, крестьяне сначала жили в обычных бараках с антисанитарными условиями. Подобные проблемы были и в других странах. В результате в США, Франции и Германии пошли по пути строительства серий домов по единому типичному проекту. Возведение подобного жилья рассматривалось за рубежом как временная вынужденная мера в условиях возросшей урбанизации.

По аналогии с западными странами, с 1955 года в Советском Союзе начала осуществляться «жилищная реформа», а на съезде КПСС в 1956 году была поставлена задача обеспечить каждую советскую семью собственной квартирой в течение следующих 15 лет.

Строящиеся дома имели стандартную внутреннюю планировку. Например, кухни и ванны были уменьшены до минимальных размеров, потолки опущены, а лифты и мусоропроводы не предусмотрены из соображений экономии. Высота подавляющего большинства хрущёвок - 4 или 5 этажей. «Хрущевки» строили более четверти века – до середины 1980-х. Основной пик пришелся на 1960-е, но уже в следующем десятилетии пятиэтажки стали уступать первенство более высоким зданиям.

Реализуя политику жилищного строительства, руководство страны исходило из принципа «Быстро, много, дёшево». Это не могло не обернуться множеством недостатков, характерных именно для «хрущёвок»: тонкие перегородки между комнатами, низкий уровень звукоизоляции, промерзание швов, протекание крыш, внешняя непривлекательность и др.

Несмотря на все изъяны, хрущевское жилье решило жилищный кризис в СССР. С начала строительства первых прототипов «хрущевок» в 1956 г. по 1963 г. жилищный фонд СССР вырос почти вдвое: с 640 млн кв. м до почти 1,2 млрд. Этот прирост по размеру был больше, чем весь объем жилья, построенного за первые сорок советских лет. К концу правления Хрущева в новые квартиры переехали 54 миллиона человек, а еще спустя пятилетку это число увеличилось до 127 миллионов [1].

Большинство ранних «хрущевок» было рассчитано на 25 лет, однако прослужили они уже более полувека. Этот возраст для многих серий панельных домов оказался критическим. «Хрущевки» сегодня по большей части стоят на пороге непригодности для жизни людей, а это примерно десятая часть жилищного фонда страны.

В связи с этим начала осуществляться политика реновации, которая подразумевает полную замену старого жилья новым. Если в странах Восточной Европы пошли по пути

надстройки и модернизации старых зданий, то в российской столице было принято радикальное решение снести все 1722 «хрущевки» первых серий, а на их месте построить современное жилье. Однако в результате на месте бывших зеленых микрорайонов появились высотки с парковками, не имеющие ничего общего с современной благоустроенной городской средой. По-прежнему отсутствуют планы по реновации «хрущёвок» в российской глубинке. В регионах спрос на «хрущевки» сохраняется, и жильцы стараются самостоятельно решить проблему реконструкции и улучшения жилищных условий путем сноса перегородок, визуального расширения пространства [2].

На данный момент в Белгородской области насчитывается около тысячи «хрущёвок», что составляет почти 30% всех многоквартирных домов. Значительная часть из них находится в Старом Осколе – около трёхсот. В последние несколько лет осуществляется благоустройство города – старые дома укрепляют, перекрашивают и в целом частично модернизируют.

С целью определения уровня осведомлённости современной молодёжи особенностями старого жилищного фонда в нашем городе, было проведено анкетирование студентов 1 курса всех специальностей общей численностью 317 человек. Респондентам было предложено ответить на четыре вопроса по теме исследования. В результате была получена следующая информация:

1. Большинство студентов (52, 68 %) проживают в новой (Северо-восточной) части города.
2. Подавляющее большинство – 61, 51 % или 195 человек – живут в домах 9 этажей и выше. В 4-х и 5-этажках – 14,2 % и 24,29 % – в домах низкой этажности.
3. Заявили, что проживают в домах хрущёвского типа почти 13 % опрошенных. При этом более 21 % испытали затруднение при ответе.
4. Лишь треть опрошенных (31,55 % или 100 человек) знают отличительные черты подобного типа жилья. Среди приведённых характеристик «хрущёвок» чаще всего встречались следующие варианты: жильё, построенное на скорую руку; аварийное жильё; дом без лифтов; компактное жильё, маленькие комнаты; лёгкое в постройке; дешёвые дома; одинаковые дома, однотипные; панельные дома; внешне непривлекательные; дефекты постройки, кривые стены.

Таким образом, «хрущёвки» - не только символ советской эпохи, но и неотъемлемая часть нашей современной истории. Решение проблемы облагораживания больших и малых городов по-прежнему является актуальным. Как и полвека назад, обеспечение населения комфортным, доступным жильём остаётся приоритетной задачей России как социального государства.

Список использованных источников

1. Антонов С. Быстро, тесно и одинаково: жилищный конвейер Никиты Хрущева https://histrf.ru/biblioteka/b/bystro-tiesno-i-odinakovo-zhilishchnyi-konvieiier-nikity-khrushchieva
2. Громова У. «Хрущевки» - попытка решения квартирного вопроса в СССР https://www.rmnt.ru/story/realty/xruschevki-popytka-reshenija-kvartirnogo-voprosa-v-sssr.353687/
3. Массовое жилищное строительство при Хрущёве https://stroyteh34.ru/massovoe-zhilischnoe-stroitelstvo-pri-hruscheve/
4. Хорошевский А. 100 знаменитых символов советской эпохи. – М.: Изд-во Фоліо, 2009. - 146 с.

РАЦИОНАЛИЗАЦИЯ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ ПРИ ВАКУУМИРОВАНИИ СТАЛИ

Парамонов Дмитрий Сергеевич, студент 3 курса
Научные руководители Долгих Антон Александрович, преподаватель
Гришина Светлана Сергеевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Как известно, одним из главнейших показателей успешного и эффективного производства является экономическая составляющая, а именно, эффективное использование имеющихся на данном производстве технических средств. Зачастую нерациональное использование имеющегося оборудования и материалов негативно отражается на экономических показателях.

Рациональное использование производственных мощностей отражается на финансовых результатах работы предприятия за счет: увеличения выпуска продукции, снижения себестоимости, улучшения качества продукции и увеличения балансовой прибыли.

В сталеплавильном производстве, наряду с процессом выплавки стали, также наиболее энергоёмким процессом является процесс обработки стали в стальковше. Этот процесс называется внепечная обработка, которая может включать в себя обработку металла на агрегате комплексной обработке стали (АКОС), обработку на установке продувки металла инертным газом и процесс вакуумирования жидкой стали.

При обработке металла вакуумом происходит колоссальные затраты электроэнергии на создание вакуума. Вакуум получают за счёт пароэжекторных насосов, для работы которых необходимо большое количество перегретого пара. Параметры работы пароэжекторного насоса и кинетики протекания реакций обезуглероживания в процессе внепечной обработки представлены в работе [2].

Вакуумная обработка металла может производится по двум режимам работы пароэжекторного насоса: экономичный режим и режим с повышенной нагрузкой. В зависимости от цели вакуумирования и сортамента стали разряжение в вакуум-камере может меняться в широком интервале – от 0,5 до 70 мм рт. ст.[1].

Кроме работы пароэжекторных насосов, в статью затрат можно отнести расход футеровочных материалов, заправочной массы для подварки патрубков ваккууматора, время на ремонт и восстановления футеровки вакуум-камеры, время на демонтаж отработанной вакуум-камеры и монтаж новой камеры, трудозатраты на текущее обслуживание установки и др.

Для того, чтобы снизить затраты целесообразно будет рационализировать процесс работы оборудования в процессе вакуумирования стали. Так как основной целью этого процесса является дегазация стали, то и оперироваться необходимо в основном на этот показатель, взяв во внимание остаточное содержание водорода, которое выражается в парциальном давлении (ppm) и зависит, в основном, от разряжения в вакуум-камере и от времени вакуумирования.

Понижение давления над жидким металлом может вызвать удаление растворенных в нем газов (водорода и азота). Кроме растворенных газов, в атмосферу могут удаляться в газообразном состоянии и металлические примеси, упругость паров которых выше давления в системе. Поэтому на разное состояние при нормальных условиях и разные формы существования в стальном расплаве газов и металлических примесей, существуют общие закономерности их удаления из расплава при вакуумной плавке или обработке стали.

Удаление газов при вакуумировании стали обусловлено уменьшением их парциального давления в атмосфере при уменьшении общего давления над сталью в результате вакуумирования [3].

Водород и азот содержатся в стали в количествах, обычно превышающих равновесные и при парциальных давлениях, достигаемых в вакуумных агрегатах, поэтому при вакуумировании имеются термодинамические предпосылки для их удаления. Однако процессы удаления в вакууме газов (водорода и азота) и металлических примесей вследствие непрерывной откачки выделяющихся газов и конденсации паров на сравнительно холодных частях установок носят ярко выраженный неравновесный характер, поэтому оценку этих процессов более правильно проводить не с точки зрения термодинамического равновесия, а с точки зрения кинетики удаления.

Основываясь на опытных данных можно вывести зависимость содержания H_2от времени вакуумирования при постоянном значении разряжения, равном 0,8-1,1mbar.

Рисунок 1 – График зависимости содержания водорода в стали от времени вакуумирования

Из графика (рис.1) видно, что основная часть H_2 (80-85%) уходит из стали за первые 12-15 минут вакуумирования, что соответствует содержанию 1,3-1,45ppm. При дальнейшей работе вакуум-камеры удаление водорода происходит незначительно.

Большинство современных предприятий, в том числе и ОЭМК, не ограничивается производством конкретных марок стали, а имеет в своей разработке различное множество марок стали. Марки стали, производимые на предприятии имеют различный химический состав, и соответственно, различную схему и способ обработки. Кроме этого, по требованию заказчиков, стали имеют разные заданные пределы по содержанию водорода. Учитывая эти требования, время обработки металла вакуумом можно производить в зависимости от заданных пределов для конкретной марки стали, рационализируя ресурс используемого оборудования.

Марки стали по содержанию водорода разделяют на различные группы, с разным содержанием водорода (не более 2 ppm, не более 2,5 ppm, не более 3 ppm, не более 4 ppm и с H_2 не более 5 ppm). Таким образом, марочник с регламентированным содержанием водорода необходимо обрабатывать вакуумом, с различным временем исходя из графика (рис.1).

На основании практических данных, марки стали можно сделать вывод что, стали целесообразно обрабатывать вакуумом при содержании водорода не более 2 ppm - 20-25 мин., при H_2 от 2,5 до 3 ppm – 15-18 мин., при H_2 более 3ppm – 10-12 мин. (табл.1).

Таблица 1 – Время обработки в вакуум-камере, в зависимости от содержания водорода в марке стали.

Содержание водорода, не более	2 ppm	2,5 ppm	3 ppm	4 ppm	5 ppm
Время вакуумирования, мин	15-20	15-18	10-12	Не более 10	Не более 10

При выборе времени вакуумирования также следует учитывать и возможный прирост содержания водорода при дальнейшей обработке согласно технологии на данную марку стали. Поэтому стоит задуматься и о минимизации обработки расплава после вакуумирования.

Таким образом, уменьшение затрат ресурса оборудования повлечёт за собой сокращение затрат на энергоресурсы, на компонующие материалы (футеровка, масса и др.), увеличит стойкость вакууматора за счёт сокращения времени контакта с агрессивной средой расплава и улучшит другие сопутствующие технико-экономические показатели.

Список использованных источников

1. Бигеев В.А., Основы металлургического производства: учебник / В.А. Бигеев, К.Н. Вдовин., В.М. Колокольцев – Санкт-Петербург: Издательство Лань-Трейд, 2017. - 616 с.
2. https://www.dissercat.com/content/issledovanie-i-razrabotka-tekhniki-i-tekhnologii-vakuumnoi-obrabotki-stali
3. http://emchezgia.ru/vakuumnaya/5.3_udalenie_gazov_i_primesyei.php [Текст]- Вакуумирование - удаение газов и летучих примесей в металлургии

АНАЛИЗ ЛИКВИДНОСТИ И ПЛАТЕЖЕСПОСОБНОСТИ ООО «МАРТЕН ПРАЙС»

Резцова Виолетта Викторовна, студент 3-го курса
Научный руководитель Дерикот Ольга Викторовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Для того, чтобы правильно и в полной мере охарактеризовать любое предприятие, необходимо оценить его финансовое состояние. Под финансовым состоянием понимается способность компании финансировать свою деятельность. Оценка финансовой состоятельности подразделяется на 5 основных блоков, среди которых находятся блок оценки показателей платежеспособности и блок показателей ликвидности. [2, с. 304]

Платежеспособность – это способность предприятия рассчитываться по платежам для обеспечения процесса непрерывного производства. Основными признаками платежеспособности являются наличие в достаточном объеме средств на расчетном счете и отсутствие просроченной кредиторской задолженности. Низкая платежеспособность означает, что компании в ближайшее время может не хватить или уже не хватает средств для того, чтобы своевременно расплачиваться по своим обязательствам. [1, с. 101-102]

Что касательно ликвидности, ликвидность – это способность активов трансформироваться в денежные средства, а именно величина, обратная продолжительности временного периода, в течение которого эта трансформация может быть осуществлена. Говоря о ликвидности компании, подразумевается наличие у нее оборотных средств в размере, достаточном для погашения краткосрочных обязательств. Ликвидность баланса - это такое соотношение активов и пассивов, которое обеспечивает своевременное покрытие краткосрочных обязательств оборотными активами. [2, с. 316]

Показатели ликвидность и платежеспособность являются взаимосвязанными и взаимодополняемыми. Например, при сопоставлении групп активов и пассивов баланса можно выявить не только соблюдение условия абсолютной ликвидности, но и наличие или отсутствие у организации текущей и перспективной платежеспособности (таблица 1). Анализ ликвидности баланса ООО «Мартен Прайс» представлен в таблице 2.

Таблица 1 – Группировка активов и пассивов. Условие абсолютной ликвидности

Актив	**Неравенство**	**Пассив**	**Значение**
А1 – абсолютно ликвидные активы – деньги, краткосрочные финансовые вложения;	А1 >= П1	П1 – наиболее срочные обязательства – кредиторская задолженности и прочие пассивы;	Текущая платежеспособность (имеется достаточный объем денежных средств для покрытия краткосрочных обязательств);
А2 – быстро реализуемые – краткосрочная дебиторская задолженность и прочие оборотные активы;	А2 >= П2	П2 – краткосрочные – краткосрочные заемные средства;	
А3 – медленно реализуемые – долгосрочная дебиторская задолженность, запасы и НДС;	А3 >= П3	П3 – долгосрочные – все долгосрочные обязательства;	Перспективная платежеспособность;
А4 – трудно реализуемые – все внеоборотные активы.	А4 <= П4	П4 – постоянные пассивы – капитал и резервы.	Необходимое условие финансовой устойчивости.

Таблица 2 – Оценка ликвидности бухгалтерского баланса ООО «Мартен Прайс», тыс. руб.

Активы			Пассивы			Платежный излишек (+) или недостаток (-)	
Группировка по степени ликвидности	На 31.12.18	На 31.12.19	Группировка по степени срочности погашения	На 31.12.18	На 31.12.19	На 31.12.18	На 31.12.19
А1 – абсолютно ликвидные активы	0	368	П1 – наиболее срочные обязательства	3434	3778	-3434	-3410
А2 – быстро реализуемые активы	1205	1057	П2 – краткосрочные обязательства	0	0	+1205	+1057
А3 – медленно реализуемые активы	2559	2729	П3 – долгосрочные обязательства	0	0	+2559	+2729
А4 – трудно реализуемые активы	0	0	П4 – постоянные пассивы	330	376	-330	-376
Итого	3764	4154	Итого	3764	4154	-	-

На основании таблиц 1 и 2 можно сделать выводы о ликвидности бухгалтерского баланса ООО «Мартен Прайс». В результате сопоставления активов и пассивов было установлено соблюдение следующих условий (как на конец 2018, так и на конец 2019 года):

А3>П3, следовательно, у организации имеется долгосрочная (перспективная) платежеспособность;

А4<П4 , следовательно, у ООО «Мартен Прайс» имеется собственный оборотный капитал, что является важным условием платежеспособности;

А2>П2, но А1<П1, так как А1+А2<П1+П2, то предприятие не имеет текущей платежеспособности.

Из чего следует, что ни на конец 2018, ни на конец 2019 года баланс ООО «Мартен Прайс» не являлся абсолютно ликвидным,.

Для оценки платежеспособности также используется ряд коэффициентов (таблица 3):

1) Коэффициент абсолютной ликвидности показывает, какая часть краткосрочных пассивов может быть погашена за счет абсолютно ликвидных активов.

2) Коэффициент критической (срочной) ликвидности показывает, какая часть краткосрочных обязательств может быть погашена за счет имеющихся денежных средств и ожидаемых поступлений от дебиторов.

3) Коэффициент текущей ликвидности позволяет оценить, в какой степени оборотные активы покрывают имеющиеся краткосрочные обязательства. [3, с. 290-291]

Таблица 3 – Анализ платежеспособности ООО «Мартен Прайс»

Показатель	Оптимальное значение	На 31.12.18 г.	На 31.12.19 г.	Отклонение (+,-)
1	2	3	4	5
Исходные данные				

1. Денежные средства и краткосрочные финансовые вложения, тыс. руб.	-	0	368	+368
1	2	3	4	5
2. Краткосрочная дебиторская задолженность, тыс. руб.	-	1205	1057	-148
3. Общая величина оборотных активов, тыс. руб.	-	3764	4154	+390
4. Краткосрочные обязательства, тыс. руб.	-	3434	3778	+344
Оценка текущей платежеспособности				
5. Коэффициент абсолютной ликвидности	0,2 – 0,3	0	0,10	+0,10
6. Коэффициент критической ликвидности	0,8 - 1,0	0,35	0,38	+0,03
7. Коэффициент текущей ликвидности	1,5 – 2,0	1,10	1,10	0

Из таблицы 3 видно, что положительная тенденция наблюдается не только со стороны абсолютных показателей, но и относительных. Изменение коэффициентов произошло в основном за счет увеличения размера денежных средств на 368 тыс. руб. Однако, несмотря на это, значения как на конец 2018, так и на конец 2019 года ниже оптимальных, что говорит о низкой платежеспособности организации. Для того, чтобы оплатить всю имеющуюся у организации кредиторскую задолженность, необходимо привлечь не только абсолютно ликвидные и быстрореализуемые активы, но и значительную часть запасов, незавершенного производства и готовой продукции.

Не меньшую роль при анализе платежеспособности организации играет отчет о движении денежных средств. На основании данной формы составляются аналитические таблицы, определяется динамика и структура денежных потоков, основные их направления, в частности рассчитываются удельные веса и абсолютные отклонения, как по всем видам деятельности, так и по каждому в отдельности. У ООО «Мартен Прийс» отсутствуют потоки от инвестиционных и финансовых операций. Анализ движения денежных средств по текущей деятельности представлен в таблице 4.

Таблица 4 – Анализ ДДС по текущей деятельности ООО «Мартен Прайс», тыс. руб.

Показатель	2018 г.	2019 г.	Отклонение (+, -)	Темп роста, %
1. Поступление денежных средств, всего	28082	25717	-2365	91,58%
1.1. Средства, полученные от продажи продукции, товаров, работ и услуг	27876	25252	-2624	90,59%
1.2. Прочие поступления	206	465	259	225,73%
2. Платежи денежных средств, всего	29249	25349	-3900	86,67%
2.1. Оплата за сырье, материалы, работы, услуги	24625	21301	-3324	86,50%
2.2. Оплата труда работников	1004	962	-42	95,82%
2.3. Платежи по налогу на прибыль	11	12	0	100,00%
2.4. Прочие платежи	3609	3075	-534	+85,20
3. Чистый денежный поток	-1167	368	1535	-31,53

Из таблицы 4 видно, что основным источником поступлений является продажа (реализация) продукции, а основным направлением платежей – оплата сырья, материалов, работ и услуг. Это является стандартной ситуацией на любом предприятии. Также из таблицы 4 видно, что в 2019 году происходит рост чистого денежного потока, что является благоприятным условием для дальнейшего развития организации и напрямую влияет на увеличение ее платежеспособности и ликвидности.

Исходя из всего вышеизложенного, следует, что для улучшения финансового положения ООО «Мартен Прайс», необходимо сократить размер кредиторской и дебиторской задолженности, что также позволит уменьшить зависимость организации от третьих лиц (кредиторов и дебиторов). В случае возникновения потребности в привлечении заемных средств, наиболее выгодными в условиях нестабильной экономики будут являться долгосрочные обязательства. Для сокращения размера имеющейся задолженности стоит уменьшить длительность её оборота, увеличив тем самым её оборачиваемость. Это позволит превратить имеющиеся обязательства в реальные денежные средства. В случае невозможности уменьшения размера задолженности, еще одним путем повышения ликвидности может стать снижение объема материалов за счет нормирования или продажи.

Список использованных источников

1. Жилкина, А. Н. Финансовый анализ: учебник и практикум для вузов / А. Н. Жилкина. — Москва : Издательство Юрайт, 2020. — 285 с. — (Высшее образование). — ISBN 978-5-534-02401-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450070/p.1 (дата обращения: 22.03.2021).

2. Румянцева, Е. Е. Экономический анализ: учебник и практикум для среднего профессионального образования / Е. Е. Румянцева. — Москва: Издательство Юрайт, 2020. — 381 с. — (Профессиональное образование). — ISBN 978-5-9916-7946-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/452238/p.1 (дата обращения: 22.03.2021).

3. Шадрина, Г. В. Основы бухгалтерского учета: учебник и практикум для среднего профессионального образования / Г. В. Шадрина, Л. И. Егорова. — Москва : Издательство Юрайт, 2020. — 429 с. — (Профессиональное образование). — ISBN 978-5-534-02782-2. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450809/p.1 (дата обращения: 22.03.2021).

ИЗ ИСТОРИИ ВЕЩЕЙ

Романов Алексей Алексеевич, Ряполов Денис Викторович, студенты 1-го курса
Научный руководитель Маликова Светлана Анатольевна, преподаватель, педагог-психолог
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Одежда является частью материальной и духовной культуры общества. С одной стороны, это материальные ценности, созданы человеком для удовлетворения потребностей, с другой — это произведения декоративно-прикладного искусства, эстетически преобразующие облик человека. Сегодня человеку необходимо понимать как назначение, так и возможность свободы применения различных форм и видов одежды. Мы исследовали историю развития одежды не только для развития кругозора, но и с практической точки зрения – знать, значит правильно пользоваться.

Одежда отражает развитие производительных сил исторического периода, климатические условия страны, национальные особенности жизни народа и его представления о красоте.

Одежда включает в себя различные виды изделий: белье, платье, обувь, и т.п. Именно одежда является выразителем социальной и индивидуальной характеристики человека, его возраста, пола, характера, эстетического вкуса. Безраздельно сливаясь с физическим обликом человека, костюм формирует его в соответствии с общественным эстетическим и нравственным идеалом.

Раскопки показывают, что одежда появилась на самых ранних этапах развития человеческого общества. Предполагая, что одежда возникла вначале как средство украшения и сословного отличия человека.

Археологи и искусствоведы утверждают также и то, что с изменением климата и образа жизни людей значительно усилилась защитная функция одежды.

Одежда прошла длительный и сложный путь, прежде чем стать столь целесообразной по форме, как сейчас.

Можно выделить несколько характерных периодов развития:

Первый период — это период развития прототипов одежды из шкуры животных, волокна растений и т. п. Он длился несколько сотен тысяч лет — примерно до V тысячелетия до н. э. Основная функция одежды в этот период — защитная. В конце этого периода человек освоил искусство плетения, прядения, началось ручное создание тканей.

Для второго периода развития одежды, длившегося более пяти тысячелетий, было характерно обертывание тела специально вытканным куском ткани. Драпированная одежда из шерстяных, хлопчатобумажных и льняных тканей получила первоначальное развитие в районах с мягким теплым климатом. Одежда представляла собой прямоугольный или овальный кусок ткани, укрепляемый тем или иным способом на фигуре человека и образующий красивые складки.

Примером такой одежды является одежда древних греков и римлян.

Начало третьего периода характеризуется появлением кроеной одежды. Этот период относят к IX в. н. э. Сначала одежду изготовляли из прямоугольных кусков ткани, соединенных швами, а позже ее стали кроить по форме фигуры человека.

Наиболее древний вид одежды, сшитой из прямоугольного куска ткани, римская туника, послужившая основой разнообразных туникообразных рубах. Этот вид одежды существует до сих пор у народов Севера, Средней Азии и др. Рубашечный покрой одежды был распространен также в средневековой Руси.

Первые попытки кроить одежду по форме тела человека возникли на Востоке, но не получили там достаточного развития. Более благоприятные условия оказались в Европе, когда у людей появилось стремление подчеркнуть костюмом красоту форм тела.

Первую систему кройки изобрел француз Мишель в 1818 г., назвав ее системой трети. В 1831 г. она была заменена родственной ей масштабной системой. Позднее появились другие системы кройки, среди которых видное место занимали пропорционально-расчетные и расчетно-мерочные, дошедшие до настоящего времени. Возникновение систем кройки повлекло за собой необходимость снятия или пропорционального расчета мерок, определяющих размеры отдельных участков одежды на чертеже. До появления систем кройки одежду кроили только по «патронам», которые являлись семейным достоянием

IV период. Специфику одежды XX в. определяет прежде всего переход к промышленному способу ее производства, пришедшему взамен многовекового портновского ремесла. Характерными особенностями XX в. являются также рождение принципиально нового типа женской одежды и быстрая смена моды.

Широкое участие женщин в производственном процессе сделало невозможным использование традиционной одежды в том виде, в каком она была в XIX в., прежде всего по функциональным соображениям.

Вывод: Одежда, возникшая первоначально в основном для защиты тела человека от неблагоприятных климатических и атмосферных воздействий, под влиянием различных исторических, социальных и экономических условий, национальных особенностей, эволюции эстетических представлений общества претерпела множество изменений, достигла большого многообразия видов и форм и стала предметом прикладного искусства.

Список использованных источников

1. http://ru.wikipedia.org/wiki/Одежда

2. http://mycelebrities.ru - Энциклопедия великих людей и идей. Находка человека из Этцальских Альп.

3. Орленко Л.В. Терминологический словарь одежды. - М.: Легпромбытиздат, 1996. - 345 с.

4. Коблякова Е.Б. и др. Конструирование одежды с элементами САПР.- М.: Легпромбытиздат, 1988.

АНТРОПОЛОГИЯ МУЗЫКИ А.Н.СКРЯБИНА

Соколов Максим Юрьевич, студент 1-го курса
Научный руководитель Брендель Виктория Петровна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

«Жизнь, свет, борьба, воля. Вот в чем истинное величие Скрябина»
В. Софроницкий

Музыка является неотъемлемой составляющей бытия человечества. В различных видах музыкальной деятельности человек находит не только источник радости, утешения, но и способ самовыражения, возможность отразить в звуке свои чувства, идеи, идеалы. Природа взаимодействия эстетических представлений и музыкального искусства испокон веков волновала человечество. По мере эволюции музыкально-эстетических воззрений изменялись не только трактовки музыки (учение об этосе, теория аффектов и т.д.), но и формы звуковой выразительности. [4]

Кризисный характер современной культуры способствует привлечению обостренного внимания к проблемам творческой деятельности художника творца. Важнейшими проявлениями этого кризиса являются отказ от традиционных форм и методов искусства, поиск новых путей художественного творчества, пристальный интерес к проблемам человека, к его мировоззрению, стремление воплотить результаты поисков в художественном произведении. Процессы, протекающие в настоящее время в области культуры, во многом перекликаются с аналогичными явлениями, имевшими место в начале XX века, когда во всех областях культуры и искусства велись непрерывные поиски новаторских путей. В контексте этих процессов среди выдающихся деятелей русской культуры выделяется фигура А.Н. Скрябина. Его поиски синтетической формы творчества, включающей в себя элементы практически всех видов искусств, во многом опередили современное искусство, только в сравнительно недавнее время, подошедшее к открытию возможности подобного синтеза. В этом, прежде всего и состоит актуальность творчества Скрябина, увидевшего в музыкальном искусстве средство не только познания, но и преображения окружающей нас действительности.

В плане музыкально-идеологической «Серебряный век» скорее был сумерками, чем возрождением, но все же в это время шло своим путем распространение музыкального просвещения по всей стране, и деятельность Русского музыкального общества на сороковом году существования стала давать заметные результаты как в области концертной, так и музыкально-педагогической. Контингент музыкально-образованных исполнителей и слушателей начинал повсюду расти.

«Серебряный век», период в истории русской культуры с 1890-х гг. по начало 1920-х гг. Границы «серебряного века» условны. Его начало в литературе совпадает с зарождением символизма, его завершением можно считать 1921 г. – год смерти А.А. Блока, самого известного поэта-символиста и год расстрела Н.С. Гумилёва, основателя акмеизма[1].

Понятие «серебряный век», в близком к современному смысле ввел в научный обиход в 1933 г. в Париже русский эмигрант, поэт и литературный критик Николай Оцуп для обозначения в основном литературных направлений начала столетия.

Это противоречивое время духовных поисков и блужданий породило целую плеяду выдающихся творческих личностей. Оно значительно обогатило все виды искусств, а также философию. На пороге нового времени начали меняться глубинные основы жизни: представления о любви и смерти, о реальности и душе.

Символизм — одно из крупнейших направлений в искусстве (в литературе, музыке и живописи), возникшее во Франции в 1870-80-х гг. и достигшее наибольшего развития на рубеже XIX - XX веков во Франции, Бельгии и России. Символисты радикально изменили не только различные виды искусства, но и само отношение к нему. Их экспериментаторский характер, стремление к новаторству, космополитизм и обширный диапазон влияний стали образцом для большинства современных направлений искусства.

В своих произведениях символисты старались отобразить жизнь каждой души — полную переживаний, неясных, смутных настроений, тонких чувств, мимолётных впечатлений. Поэты-символисты были новаторами поэтического стиха, наполнив его новыми, яркими и выразительными образами. Символизм различает два мира: мир вещей и мир идей. Символ становится неким условным знаком, соединяющим эти миры в смысле, им порождаемом. В любом символе есть две стороны — означаемое и означающее. Вторая эта сторона повернута к ирреальному миру. Искусство — ключ к тайне. [2]

Понятие и образ Тайны, таинственного, мистического проявляется как в романтизме, так и в символизме. Однако у символистов подлинное Бытие, «истинно-сущее» или Тайна — есть абсолютное, объективное начало, к которому принадлежат и Красота, и мировой Дух.

Представители творческой интеллигенции, подвергая критическому осмыслению существовавшие ранее художественные принципы, искали иных способов освоения мира. Одни верили, что могут обрести непосредственный, ничем не осложненный взгляд на натуру.

Русский символизм заявил о себе настойчиво и внезапно. В 1892 году в журнале «Северный вестник» была опубликована статья Дмитрия Мережковского «О причинах упадка и о новейшем течении в современной русской литературе». Долгое время она считалась манифестом русских символистов.

Скрябин хотел видеть за предпринимаемым им экспериментом проявление закона высшего единства управляющего всем и вся. В своем видении музыки он исходил из врожденной психофизиологической способности цветового восприятия звуков, которая всегда индивидуальна и неповторима. В этом заключается противоречие светомузыкального замысла Скрябина и трудности его воплощения. Они усугубляются также тем обстоятельством, что композитору представлялся более сложный, не сводимый к простому освещению пространства, изобразительный ряд.

При жизни Скрябина реализовать световой проект не удалось. И дело было не только в технической неподготовленности этого эксперимента: сам проект заключал в себе серьезные противоречия. Что же касается инженерно-технической инициативы, то ей суждено было сыграть немаловажную роль в будущей судьбе «световой симфонии» и светомузыки в целом.

Совершенно очевидно, что русская культура начала XX века воспринимала Скрябина с его философской концептуальностью и ярко выраженным стилем как художественно экстраординарное явление. Революционные деятели высоко оценили музыку Скрябина, прежде всего, в связи с ее обращенностью к миллионам и энергетическим духовным потенциалом. Однако записи самого композитора свидетельствуют о духовной проекции его музыкально-философских замыслов. [5]

Нынешняя эпоха с её новаторскими изобретениями и творческим подходом подарит человечеству в абсолютно новом видении и воплощении произведения А.Н. Скрябина «Поэма огня», «Прометей» и другие.

Рис. 9 Фортепиано в цвете.

Многим известна считалочка, которая помогает запомнить все цвета радуги: «Каждый охотник желает знать, где сидит фазан». А что, если придать музыкальным тональностям свою окраску? Возможно ли это? Да, это действительно реально. На самом деле раскрасить музыкальную радугу очень просто, главное взять нужный цвет и начать рисовать. Для этого нужно помнить тональность. Так что же такое музыкальный окрас? Какие цвета нужно использовать для обозначения звуков? Да и существует ли подобное соответствие музыкальных звуков цветам?

Прежде чем познакомить читателя с цветотональностью, нужно сказать, что музыкальная краска представляет собой не просто отдельные звуки и цвета, а целую последовательность, то есть определённую цепочку, другими словами – музыкальную гамму. Гамма образует лады, мажор, минор и тональность. Кстати, в слове «тональность» есть корень «тон», который используется как в музыке, так и в живописи.

Первым, кто предложил использовать цветотональность, был Александр Николаевич Скрябин. Благодаря своему уникальному звуко-музыкальному слуху, он создал целую систему, позволяющую определять цвет в зависимости от тональности звука.

Интересен тот факт, что первые тональности полностью повторяют цветовую гамму радуги, а что касается остальных, то они являются производными. Более того, композитор предложил использовать разделение тональностей на «духовные», к которым отнёс фа-диез мажор, а также «земные» и «материальные», к которым относятся до-мажор и фа-мажор. Аналогично тональностям, композитор охарактеризовал цвета, например, красный символизировал «цвет ада», а фиолетовый и синий – цвет «духовности» или «разума». Слушать радио Европа плюс онлайн на plus-music.org

Вместе с созданием такой цветотональности, композитор Скрябин совместил музыкальное выступление со световой партитурой. Так, например, он впервые в 1910 году создал музыкальное произведение «Прометей», которое использовало не только симфонические переходы, но и партию цвета – Luce. В этом произведение отражались не только музыкальные части, но и всевозможные эпизоды цветовых форм. [3]

В основу своей системы цветотональности, Скрябин заложил утверждение, что все, кто обладает подобным цветовым слухом, воспринимают цвета и звуки так же, как и он. Однако оказалось, что он ошибался. Другие композиторы, обладающие таким же уникальным слухом, воспринимали звуки и соотносили их с цветами совсем по-другому. Например, Римский-Корсаков, видел до-мажор белого цвета, а соль-мажор – коричневым. Кроме того, ми-мажор и ми-бемоль мажор ассоциировались у него с сапфировым и тёмно сумрачным цветами соответственно.

Фонтаны нового поколения интересны благодаря новым достижениям и открытиям современной эпохи.

Например, музыкально – световые погружают нас в волшебный мир огней, воды и музыки.

Пражские достопримечательности сложно пересчитать по памяти. Сам город – это один большой памятник архитектуры, скульптуры и т.д. Если расспросить туристов, какие места они любят посещать в столице Чехии, то большинство, в первых числах, назовёт поющие фонтаны Праги, которые поистине являются чудом.

Пылкие чувства к фонтанам у чехов совершенно не случайны. Иоганн Кеплер – известный чешский учёный, работавший при дворе Рудольфа II в Праге. Именно он стал творцом насоса шестеренчатого для императорского фонтана. Эта разработка до сих пор

лежит в основе функционирования фонтанов. Но вот что касается названия, то первый чешский «поющий фонтан» находится в Пражском Граде (в Королевском саду). Да и время его создания ещё более впечатляющее – 1574 год. Но почему же фонтан поющий? Да потому что вода, падающая вниз, попадала на металлические диски и издавала звук, похожий на звук колоколов, то есть их «пение».

Создателем поистине волшебных поющих фонтанов стал изобретатель, инженер Франтишек Кржижик. Это имя фонтаны носят и сегодня – Кржижиковы фонтаны. Фантазия изобретателя была сильна, ведь он, в далёком 1891 году усилил сооружение электрической подсветкой. Так фонтаны заиграли с новой силой. И не просто заиграли! Спустя сто лет была произведена реконструкция фонтанов: они были компьютеризированы, благодаря чему стали возможны не просто игра цвета, воды и музыки, но и создание целых представлений.

Кржижиковские фонтаны в Праге (Křižíkova fontána) — цветомузыкальные фонтаны, ставящие красочные театральные шоу. Красивейший пражский аттракцион является детищем Франтишека Кржижика. Фонтаны бьют струями воды разной силы в такт цветомузыке на фоне, теряющегося в темноте, здания Дворца промышленности. Ежедневно проходит четыре представления.

В репертуар Кржижиковских фонтанов включены произведения мировой классики, мюзиклы, различные поп и рок-хиты современной мировой эстрады. На фоне фонтанов часто разыгрываются различные постановки классического и современного балетов, а с 2001 устраиваются мультимедийные шоу, когда на экран, создаваемый струями воды, проецируются видео ролики.

Если бы нынешняя эпоха с её новаторскими изобретениями и творческим подходом, то «Поэма огня», «Прометей» А.Н. Скрябина нашли бы воплощение в абсолютно новом видении…

Нынешняя эпоха с её новаторскими изобретениями и творческим подходом подарит человечеству в абсолютно новом видении и воплощении произведения А.Н. Скрябина «Поэма огня», «Прометей» и другие.

Список использованных источников

1.Маслякова А.И. Принцип всеединства и его преломление в творчестве А.Н. Скрябина // Музыковедение. — М.: Изд-во «Научтехлитиздат». — 2010. — № 12. — С. 23–27

2.Маслякова А.И. Мистицизм А.Н. Скрябина в контексте русского космизма // Музыка и время. — М.: Изд-во «Научтехлитиздат». — 2012. — № 3 (март). — С. 32–35 3. А.Н. Скрябин. Любовь и музыка. – М.: Ирис-пресс, 1993. Ч. 2. – 1993 – 24 С.

4. Никитина В.П. А. Н. Скрябин. Русский композитор и пианист. – Спб, 1991, стр. 87 – 156.

5.Маслякова А.И. Время в музыке и время жизни // Музыкальная психология и психотерапия. — М.: Изд-во ГКА им. Маймонида.— 2010. — № 1 (16). — С. 24–31

МЕЖЛИЧНОСТНЫЕ ОТНОШЕНИЯ В СТУДЕНЧЕСКОЙ ГРУППЕ

Стыценко Артем Денисович, студент 2 курса
Научный руководитель Масалытина Оксана Витальевна, преподаватель, к.э.н., доцент
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Студенческий возраст представляет собой особый период жизни человека, переходный от юности к зрелости. Юношеский («студенческий») возраст, юношеский период - это начало самостоятельной, взрослой жизни. В юношеском возрасте выделяются следующие возрастные периоды: 16-17 лет - ранняя юность, 17-20 лет - собственно юность, 20-21 год - поздняя юность [1]. Эти возрастные периоды имеют свою специфику, но, при этом, обладают многими общими характеристиками.

Межличностные отношения студентов обуславливаются, во-первых, возрастными особенностями данной социальной группы, во-вторых, особенностями присущей ей деятельности. Профессиональная подготовка в образовательной организации проходит на основе вовлечения будущего специалиста в такие виды деятельности как учебная, научно-исследовательская и общественная деятельность. Учебная деятельность выступает основным видом деятельности студента, занимающим наибольший объем времени во всем процессе подготовки будущих специалистов. Научно-исследовательская деятельность исполняется в процессе участия в работе различных научных сообществ и объединений. Общественная работа позволяет значительно обогатить социальный опыт студентов в сфере построения межличностных взаимодействий, сформировать у них позитивные личностные черты. В период обучения студенты проявляют себя также в эстетической и досуговой видах деятельности, которые в случае их положительной направленности оказывают позитивное влияние на личностно-профессиональное развитие молодых людей, позволяют существенно обогатить содержание их межличностного взаимодействия.

Среди множества факторов - экономических, политических, культурных и т.д. - высоко значимой для построения и развития межличностных отношений студентов выступает среда, формируемая в рамках колледжа. Образовательная среда включает в себя ряд структурных единиц, оказывающих влияние на личность. Она может включать: физическое окружение (архитектура здания, размеры, находящихся учебных помещений и т.д.); человеческие факторы (личностные, статусно-ролевые, возрастные, национальные и иные особенности обучающихся); программы обучения (стиль преподавания, особенности контроля и оценки и т.д.). Несмотря на прослеживающееся влияние всех обозначенных структурных единиц образовательной среды на межличностные отношения студентов, в качестве ведущих для их построения в психологии рассматривается человеческий фактор.

Студенческая академическая группа является первой и основной ячейкой, где формируется личность будущего специалиста, это сложное и многообразное социальное явление, которое развивается по объективно существующим законам, законам общения. Мощное социализирующее воздействие на личность студента оказывает сама студенческая среда, особенности студенческой группы, в которую входит человек, особенности других референтных групп. В студенческой группе происходят динамичные процессы структурирования, формирования и изменения межличностных, эмоциональных и деловых взаимоотношений, распределения групповых ролей и выдвижения лидеров и т.п. Все эти групповые процессы оказывают сильное влияние на личность студента, на успешность его учебной деятельности и профессионального становления, на его поведение. Такие особенности студенческой группы, как однородность возрастного состава (разница в возрасте обычно не более 2 лет), обуславливает возрастное сходство интересов, целей, психологических особенностей, способствует сплочению группы.

Основной вид деятельности студенческой группы - учение, а факторы учебного сплочения слабее, чем производственные, поэтому порой сплоченный коллектив не складывается: каждый сам по себе. Студенческие группы функционируют как на основе самоуправления через систему формальных и неформальных лидеров, так и подвергаются определенным управляющим воздействиям со стороны преподавателя. В студенческой группе проявляются такие социально-психологические явления, как:

- «коллективные переживания и настроения»-эмоциональная реакция коллектива на события в коллективе, в окружающем мире; коллективное настроение может стимулировать или угнетать деятельность коллектива, приводя к конфликтам, может возникать настроение оптимистическое, безразличное или неудовлетворенности;
- «коллективные мнения» - сходство суждений, взглядов по вопросам коллективной жизни, одобрение или порицание тех или иных событий, поступков членов группы; явления подражания, внушаемости или конформизма, явления соревнования - форма взаимодействия людей, которые эмоционально ревностно относятся к результатам своей деятельности, стремятся добиться успеха.

Межличностные отношения связывают, прежде всего, студентов с друг другом. Отношения типа «студент-студент» в студенческой среде относятся к горизонтальному уровню взаимодействия, которое характеризуется интенсивностью неформального общения, удовлетворением психологических потребностей, формированием черт характера и свойств личности. Отношения между студентами представляют собой форму взаимодействия со сверстниками, пропитанную специфическими задачами профессионализации. Общение со сверстниками в студенческом возрасте продолжает выступать средством усвоения молодыми людьми статусов и ролей, отработки коммуникативных навыков и стилей общения в новой социальной среде. Важно также и то, что данное общение выступает разновидностью эмоционального контакта, способствующей осознанию группой своей принадлежности, автономии, эмоционального благополучия и устойчивости.

Качество межличностных отношений студентов во многом определяется уровнем развития студенческой группы. Являясь одной из разновидностей социальных групп, студенческая группа развивается по объективно существующим законам общества, но обладает и некоторым своеобразием и неповторимостью. Среди особенностей студенческой группы, влияющих на устанавливаемые в ней межличностные отношения можно выделить следующие:

- цель, состоящая из овладения знаниями, умениями, навыками и подготовки к профессиональной деятельности;
- учеба как основной вид деятельности;
- индивидуальные формы труда;
- отсутствие отношений «по вертикали»;
- относительная возрастная однородность;
- ограниченность периода существования.

Развитие студента на различных курсах имеет некоторые особые черты. Первый курс решает задачи приобщения недавнего абитуриента к студенческим формам коллективной жизни. Поведение студентов отличается высокой степенью конформизма; у первокурсников отсутствует дифференцированный подход к своим ролям. Второй курс - период самой напряженной учебной деятельности студентов. В жизни второкурсников интенсивно включены все формы обучения и воспитания. Студенты получают общую подготовку, формируются их широкие культурные запросы и потребности. Процесс адаптации к данной среде в основном завершен. Третий курс - укрепление интереса к научной работе как отражение дальнейшего развития и углубления профессиональных интересов студентов. Для поведения студентов характерен интенсивный поиск более рациональных путей и форм специальной подготовки, происходит переоценка студентами многих ценностей жизни и культуры. Четвертый курс - перспектива скорого окончания колледжа формирует четкие практические установки на будущий род деятельности. Проявляются новые, становящиеся

все более актуальными ценности, связанные с материальным положением, местом работы и т.п.

Студенческий возраст, в котором пребывают члены группы - это пора достижений, стремительного накапливания знаний, умений, становления нравственности, обретение новой социальной позиции. В это же время, юношеский возраст характеризуется потерей детского мироощущения и наступает пора сомнений в собственных силах, возможностях, утверждение собственного «Я« в обществе, и взаимоотношений с окружением. На этой почве отношение к коллективу меняется по сравнению со школьными годами, наблюдается избирательность в межличностном общении, критичность по отношению к коллективу. Активность и процесс утверждения своего «Я» среди сверстников затрудняется тем, что он осуществляется на основе однотипных профессиональных интересов [2].

Таким образом, знание психологических особенностей студенческого возраста на современном этапе становится очень важным и необходимым явлением в психологии. Становление личности студента происходит в группе, которая находится на определенном этапе своего развития. Характер развития личности в значительной мере обусловлен уровнем развития группы, в которую личность включена и в которой она интегрирована. В академических группах, которые достигли в своем развитии уровня коллектива, существуют благоприятные условия для формирования у студентов положительных качеств личности, необходимых современному специалисту.

Список использованных источников

1. Сапогова, Е.Е. Психология развития человека / Е.Е. Сапогова. - М., 2001.
2. Педагогика и психология высшей школы / Под ред. Юсупянц Э.А. - Ростов н/Д., 2002.

АНАЛИЗ ФИНАНСОВЫХ РЕЗУЛЬТАТОВ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ НА ПРИМЕРЕ ООО «КАРАВАЙ»

Фатеева Анастасия Владиславовна, студент 3 курса
Научный руководитель Дерикот Ольга Викторовна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Анализ финансовых результатов представляет собой один из наиболее существенных элементов экономического анализа, занимая достаточно важное место в принятии решений по управлению финансами организации. [2, с. 3]

Финансовый анализ – это наука о сфере человеческой деятельности, направленной на изучение, теоретическую систематизацию, объяснение и прогнозирование процессов, которые происходят с финансовыми ресурсами и их потоками, через оценку финансового состояния выявленных возможностей совершенствования функционирования и эффективного управления как на уровне отдельного предприятии, так и на государственном уровне. [1, с. 11]

Проведение финансового анализа компании требует использования различных документов, статистической и финансовой отчетности хозяйствующего субъекта, годовых отчетов руководителей. Особое внимание должно уделяться качеству и достоверности используемой информации. Организация финансового анализа в условиях наличия электронных информационных ресурсов и автоматизированных управленческих систем требует изучения опыта, а также возможностей, которые приобретают компании в результате использования современных информационных технологий в анализе. Большинство российских компаний начинают процесс автоматизации информационного пространства с бухгалтерии. [3, с. 10]

Тема работы является актуальной поскольку в условиях рыночной экономики эффективность финансовой и производственной деятельности выражается в финансовых результатах. Также в условиях рыночной экономики управление финансовыми результатами занимает центральное место в деловой жизни хозяйствующего субъекта.

Если финансовый результат положительный, то это свидетельствует о том, что эффективно используются активы организации.

В данной работе цель – проанализировать финансовые результаты деятельности ООО «Каравай».

Предметом исследования являются бухгалтерский баланс и отчёт о финансовых результатах.

Объект исследования – ООО «Каравай», основным видом деятельности которого является деятельность автомобильного грузового транспорта.

Анализ финансовых результатов организации начинается с изучения объема, состава, структуры и динамики прибыли (убытка) до налогообложения в разрезе основных источников её формирования, которыми являются прибыль (убыток) от продаж и прибыль (убыток) от прочей деятельности, т. е. сальдо всех остальных доходов и расходов.

Таблица 1 — Анализ прибыли до налогообложения ООО «Каравай»

Наименование показателя	2018 г., тыс.руб.	2019 г., тыс.руб.	Отклонение		Удельный вес		Отклонение удельного веса, %
			тыс.,руб.	% роста к 2018 г.	2018 г., %	2019 г., %	
Прибыль от	1 180,00	2 952,00	1 772,00	150,17	100	100	0

продаж							
Сальдо прочих доходов и расходов	–	–	–	–	–	–	–
Прибыль до налогообложения	1 180,00	2 952,00	1 772,00	100	100	100	0

Исходя из таблицы 1, можно сделать вывод о том, что в ООО «Каравай» прибыль до налогообложения в 2018 году составила 1 180,00 тыс.руб., а в 2019 - 2 952,00 тыс. руб. Она увеличилась на 1 772,00 руб. за счет увеличения выручки в 2019 году. Прибыль от продаж в 2018 году составила 1 180,00 руб., а в 2019 - 2 952,00 руб., т.е. показатель возрос на 1 772,00 руб. или на 50,17%.

Поскольку качество прибыли (убытка) до налогообложения определяется ее структурой, то целесообразно обратить особое внимание на изменение удельного веса прибыли от продаж в прибыли до налогообложения. Его снижение рассматривается как негативное явление, свидетельствующее об ухудшении качества прибыли до налогообложения, так как прибыль от продаж является финансовым результатом от текущей (основной) деятельности предприятия и считается его главным источником средств. Поэтому желательно следующее соотношение темпа роста прибыли от продаж (ТРпр) и темпа роста прибыли до налогообложения (ТРпдн):

$$ТРпр \geq ТРпдн. \quad (1)$$

Данное соотношение темпов роста отражает ситуацию, в которой удельный вес прибыли от продаж в прибыли до налогообложения, как минимум, не уменьшается, а, следовательно, качество прибыли до налогообложения, по меньшей мере, не ухудшается. Далее анализируются основные источники формирования прибыли (убытка) до налогообложения: прибыль (убыток) от продаж и прибыль (убыток) от прочей деятельности – в отдельности. [2, с. 18]

Анализ чистой прибыли (убытка) ведется в разрезе определяющих ее элементов, которыми являются прибыль (убыток) до налогообложения, текущий налог на прибыль, изменение отложенных налоговых обязательств, изменение отложенных налоговых активов и прочее. В ходе анализа изучается ее объем, состав, структура и динамика. Аналитические расчеты оформляются в виде таблицы.

По итогам расчетов делается вывод по поводу изменения объема, состава и структуры чистой прибыли (убытка), а также о влиянии на отклонение суммы чистой прибыли (убытка) изменений величин определяющих ее элементов: текущего налога на прибыль, изменения отложенных налоговых обязательств, изменения отложенных налоговых активов и прочего. [2 с. 20-21]

На основании данных ООО «Каравай» была проанализирована динамика факторов формирования чистой прибыли организации, которая приведена в таблице 2.

Таблица 2 — Динамика факторов формирования чистой прибыли ООО «Каравай»

Показатель	2018 г., тыс.руб.	2019 г., тыс.руб.	Отклонение (+), (-), тыс.руб.	Темп роста, %
Выручка	75 695,00	684 900,00	+ 609 205,00	904,82
Себестоимость	74 515,00	681 948,00	+ 607 433,00	915,18
Валовая прибыль	1 180,00	2 952,00	+ 1 772,00	249,75
Прибыль от	1 180,00	2 952,00	+ 1 772,00	249,75

продаж				
Прибыль до налогообложения	1 180,00	2 952,00	+ 1 772,00	249,75
Текущий налог на прибыль	236,00	590,00	+ 354,00	250
Чистая прибыль	944,00	2 362,00	+ 1 418,00	250,21

Исходя из таблицы 2, можно сделать вывод о том, что в ООО «Каравай» в 2019 году по сравнению с 2018 годом чистая прибыль увеличилась на 1418 тыс. руб. или на 50,21%. Это явилось следствием увеличения прибыли до налогообложения на 1772 тыс.руб. или на 149,75%.Поскольку в условиях ООО «Каравай» прибыль до налогообложения полностью формируется за счёт прибыли от продаж (отсутствуют прочие доходы и прочие расходы), то рост данного показателя обусловлен прежде всего увеличением выручки на 609205 тыс. руб.(на 804, 82%). Несмотря на то, что себестоимость при этом также увеличилась на 607433 тыс. руб. или на 815, 18%, был обеспечен прирост валовой прибыли на 1772 тыс. руб. или на 149, 75%. По сравнению с 2018 годом на предприятии произошёл значительный прирост прибыли, что безусловно, заслуживает положительной оценки. Тем не менее, на предприятии, имеются неиспользованные резервы роста финансовых результатов, которые прежде всего связаны с получением доходов от прочей деятельности и с более эффективным использованием имеющихся ресурсов, т.к. темпы роста себестоимости (915,18%) опережают темпы роста выручки (904,82).

Список использованных источников

1.Жилкина, А. Н. Финансовый анализ: учебник и практикум для вузов / А. Н. Жилкина. — Москва: Издательство Юрайт, 2020. — 285 с. — (Высшее образование). — ISBN 978-5-534-02401-2. — Текст: электронный // ЭБС Юрайт [сайт]. с. 11 — URL: https://urait.ru/bcode/450070/p.11.

2.Иванова, Н.В. Основы анализа бухгалтерской отчётности: учебник / Н.В. Иванова, К.В. Иванов. – 2-у изд., перераб. и доп. – Москва: КНОГРУС, 2019. – 204 с.

3.Казакова, Н. А. Финансовый анализ в 2 ч. Часть 1: учебник и практикум для вузов / Н. А. Казакова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2021. — 297 с. — (Высшее образование). — ISBN 978-5-534-08792-5. — Текст: электронный // ЭБС Юрайт [сайт]. с. 10 — URL: https://urait.ru/bcode/475006/p.10

СОЦИАЛЬНАЯ АДАПТАЦИЯ ЛИЧНОСТИ В ДИЛОГИИ «KBAZИ» - «КАЙНOZOЙ» СЕРГЕЯ ЛУКЬЯНЕНКО

Феоктистов Егор Дмитриевич, студент 1-го курса
Научный руководитель Капустина Ирина Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Сергей Лукьяненко — явление в мире фантастики уникальное и неповторимое, потому что впервые в истории жанра рамки, приемы, декорации фэнтези наложились на русскую классику.

В дилогии «Kbazи» С. Лукьяненко речь идет о планете Земля после массовой катастрофы, в ходе которой в людях пробудился ген, отвечающий за перерождение. В ходе этого перерождения человек становится зомби, т.е. полностью теряет разум и все, что у него остается - это животные инстинкты.

Если такой зомби съест кусок человеческого мозга, он станет kbazi, т.е. сильнее, гибче, быстрее, но теряет возможность есть пишу животного происхождения. Даже краситель красного цвета, производимый из жучков, вызывает рвотный позыв. Также такие «сверхлюди» застревают на том уровне развития, на котором были до первой смерти, т.е. если человек умирает в детском возрасте, то все, что ему будет интересно - это игры, если умирает медик - то полицейским он стать не сможет, если он слушал классическую музыку, то hard rock ему не понравится. Одним словом, kbazi теряют способность к саморазвитию.

На наш взгляд, люди крайне быстро приспособились к новым правилам и порядкам. За считанные месяцы люди вновь вернули цивилизованный образ жизни, но не везде. В России Москву заняли люди и малое количество kbazi, в Петербурге – наоборот; о других городах подробно не рассказывалось [1].

Первая книга повествует о Москве, в которой расследуется преступление - простому дознавателю приходится работать с kbazi. «Если вдруг вы видите мертвого человека, у вас умерла бабушка или дедушка, вы должны связать труп, заткнуть рот кляпом и позвонит в полицию», - этому учат детей в школах. Впоследствии зараженный отправится в заповедник до последующего перерождения, тайна которого строго скрывается.

Подавив массовые беспорядки, люди построили крайне гибкую систему, в которой каждая форма жизни имеет место быть. При первом прочтении романа поражает то, как быстро люди подстроились под ситуации, но, размышляя на эту тему, читатель понимает, что это более чем возможно даже сейчас [2].

Ежедневно в мире происходят катасрофы как маленькие так и крупые, и люди, пробуя разные методы, решают эту проблему, на это уходят дни или недели, гибнут тысячи. В этом цикле книг проблема решилась примерно за год, а погибли миллионы. Пропорция складывается, и это доказывает, что человек -крайне гибкое существо.

Во второй книге рассказывается о Петербурге, те же главные герои с уже более теплыми отношениями. Тут нам показали эту вселенную с изнанки, теперь мы в мире kbazi, тут другие порядки. Теперь kbazi не мертвые, а абсолютная форма жизни - так считают те, кто поглупее. Кто поумнее, видит и плюсы, и минусы этой формы жизни. Живые подростки подкрашивают кожу в синеватый оттенок, как у подростков kbazi, неживые подростки используют тональный крем, тем самым подчеркивая толерантное отношение к kbazi в их городе. Это своебразнная псевдоутопия. Но погружаясь глубже в сюжет романа, все кажется не таким радужным.

Дети совершают самоубийство в надежде переродиться в kbazi. Если вдруг ты будешь обороняться и убьешь зараженного (чему само собой все научились), то тебя сочтут негодяем, ведь ты убил потенциально разумное существо, еще и срок дадут. Да и глава мертвых, Председатель, тоже нечист душой.

Но даже в этой антиутопии поражаешься тому, как четко работает система. В барах сидят смешанные компании, на улицах разные парочки, все кругом разных форм жизни, и это поражает. В этом городе все не так, как в Москве, но это не значит, что тут плохо, но это не для всех однозначно, ведь многие помнят, кем были эти квazи раньше и кто лишил их близких и родных. В таких мелочах и показано, как поменялись законы и моральные устои людей.

На наш взгляд, эти романы крайне реалистично рассматривают решение такой проблемы, как Апокалипсис. И, когда, казалось бы, надежды нет, человек сможет приспособиться, подстроиться под систему, даже под природу и сможет обернуть все в свою сторону.

Мы все способны совершить бескорыстные поступки и в то же время выгодные для нас деяния. Ведь если взглянуть на человека с одной стороны, он будет милосерден, великодушен…а если с другой стороны? Сможем ли мы увидеть те же качества?

Список использованных источников

1. Невский, Б.: Утопия и антиутопия. / Б. Невский. - «Мир Фантастики». - № 49. - сентябрь 2007. [Электронный ресурс]. – Режим доступа: http://www.mirf.ru.
2. Семенов, С. П.,: О болезнетворных (= патогенных) явлениях и течениях в основных направлениях литературы: Фантастическая литература. / С.П.Семенов. [Электронный ресурс]. – Режим доступа: http://lib.authentism.ru.
3. Филиппов, В.: Сергей Лукьяненко: писатель. / В. Филиппов. - «Мир Фантастики». - № 8. - апрель 2004 [Электронный ресурс]. – Режим доступа: http://www.mirf.ru.

КЛАССИКИ ЛИТЕРАТУРЫ И БЕЛГОРОДЧИНА

Шраменко Анжелика Дмитриевна, студент 1-го курса
Научный руководитель Левченко Татьяна Николаевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В жизни каждого человека есть величайшая ценность – его Родина. Это понятие емкое и глубокое. *Россия, Белгородчина, Старооскольe…*

Важнейшим определяющим качеством личности любого человека является любовь к Родине. Патриотизм – самое широкое, всеобъемлющее и глубокое чувство, для менталитета русских людей оно является одной из важнейших ценностей. Быть патриотом – значит быть неотъемлемой частью Родины, помнить о своих «корнях», знать историю своего народа, изучать культурное наследие края и др.

Главное достояние Белгородской области -трудолюбивые и любящие свою землю люди. Белгородскую землю прославили видные деятели культуры, талантливые организаторы народного хозяйства, выдающиеся спортсмены и др. Белгородчина – край, где родились, жили и писали литераторы, чьи имена и творчество известны всему читающему миру: Николай Страхов, Надежда Кохановская (Соханская), Василий Ерошенко, Адриан Топоров, Арнольд Гессен, Филипп Наседкин многие другие. *Бывали в нашем краю и всемирно признанные классики литературы.*

Цель нашей работы -выявить в биографиях известных писателей и поэтов события, связанные с Белгородской областью.

В ходе исследования было проведено анкетирование среди студентов 1 курса в количестве 48 человек с целью выяснения степени знакомства с творчеством и личностями наших земляков, поэтов и писателей Белгородского края, или известных классиков литературы, как-либо связанных с нашим краем.

Опрос показал, что 94% опрошенных не знают имен поэтов и писателей, прославивших Белгородчину.

Никто из анкетируемых не смог ответить на вопрос «Известны ли вам какие-либо происходившие в Белгородской области события, связанные с творчеством, биографией известных (или малоизвестных) писателей и поэтов?»

*Однако 85% респондентов хотели бы изучать творчество поэтов и писателей Белгородчины на занятиях, поэтому тема работы актуальна. Д*анное исследование может быть полезно всем интересующимся литературным краеведением, тем, кому небезразлична судьба нашей земли.

Афанасий Афанасьевич Фет

Великий русский поэт-лирик часто гостил в Новой Таволжанке. Поэт был женат на Марии Боткиной, сестре владельцев сахарного завода, близко дружил с одним из братьев – литературным критиком и публицистом Василием Боткиным. Поэтому, бывая в своём имении Воробьёвка в Щигровском уезде (сейчас это Курская область), Фет старался навестить родственников. Например, в письме от 3 мая 1889 года поэт упоминал:«Через неделю по приезде нашем в деревню мы поехали на восток от Белгорода к Боткиным на их сахарный завод»

Михаил Афанасьевич Булгаков

Великий прозаик. В октябре 1928 года Михаил Булгаков выехал из Москвы в Тифлис. Дорога оказалась тяжелой, о чём писатель пишет в письме своей жене Любови Белозёрской:«Дорогой Любан, я проснулся от предчувствия под Белгородом. И точно: в Белгороде мой международный вагон выкинули к чёрту, т. к. треснул в нём болт. И я еду в другом, немеждународном вагоне. Всю ночь испортили…»

Это недоразумение позже было упомянуто в бессмертном романе писателя «Мастер и Маргарита»*: «Некоего гражданина сняли с севастопольского поезда связанным на* ***станции Белгород****».*

Константин Дмитриевич Бальмонт

Самый солнечный поэт русской литературы. В 1901 году Константину Бальмонту было запрещено проживать в столице и в крупных городах за участие в демонстрациях. Поэту с семьёй пришлось уехать в усадьбу Сабынино Курской губернии (современный Яковлевский округ), где жили родственники его жены князья Волконские.

Дни поездки поэт чаще всего коротал за работой над новой книгой стихов «Будем как солнце». Из Сабынино К. Бальмонт писал письма Горькому, Чехову, Толстому, Брюсову.

Аркадий Петрович Гайдар

Классик детской литературы. Весну 1934 года Аркадий Гайдар провёл в Ивне – здесь он навещал сына Тимура и бывшую супругу Лию Соломянскую. В Ивне Гайдар закончил вторую часть повести «Синие звёзды», работал над «Бумбарашем». Так Маруся из рассказа «Голубая чашка» мечтала убежать **в Белгород**, а Семён Бумбараш оказался солдатом Белгородского полка.

Александр Трифонович Твардовский

Известный поэт. Мало кто знает, что первые главы всенародно любимой поэмы А. П. Твардовского «Василий Тёркин» были написаны именно в Валуйках, где находилась редакция газеты «Красная армия».«С того времени, как в печати появились главы первой части «Тёркина», он стал моей основной и главной работой на фронте», - писал Александр Трифонович.

Игорь Андреевич Чернухин

Белгородец, родился в посёлке Томаровка. Имя поэта занесено в энциклопедию «Лучшие люди России». Одна из улиц посёлка городского типа Томаровка носит имя поэта. Изучение творчества вошло в программу предмета «Родная литература» в школах Белгородской области.

Василий Яковлевич Ерошенко

Был уникальным человеком. Будучи незрячим с раннего детства, он овладел двенадцатью языками и стал профессором Пекинского университета. Был известен, как знаток японской литературы. Интересен и его дом,находящийся в селе Обуховке, который является памятником архитектуры.

Николай Николаевич Страхов

Для Николая Николаевича Страховарусского философа, публициста, литературного критика, первого биографа Ф. М. Достоевского, близкого друга Л.Н.Толстого, Белгород был родным домом.

Евгений Александрович Евтушенко

Русский поэт, прозаик, режиссёр, публицист. Был номинирован на Нобелевскую премию по литературе. 3 июня 2010 г. в Старооскольском театре для детей и молодежи состоялась встреча с известным поэтом - шестидесятником. Со сцены прозвучало стихотворение «Не стало поэта…», которое было написано в поезде по дороге в Старый Оскол и посвящено памяти А. Вознесенского. В нашем городеЕвгений Евтушенко стал зрителем на концерте-спектакле режиссёра Семёна Лосева «Женя, а вы знаете…» по произведениям поэта.

Гарий Леонтьевич Немченко

В Старый Оскол из Москвы известный русский писатель, публицист, переводчик, общественный деятель Гарий Леонтьевич Немченко в январе 2015 года прибыл для участия в большой читательской конференции, посвященной его документальному роману «Бригадир» (*о нашем знаменитом земляке, главе администрации города Старый Оскол и Старооскольского района Николае Петровиче Шевченко).*

Сегодня, в век всемирной глобализации, падения нравственности и морали особенно важно помнить о тех одаренных людях, которые незаметно жили рядом с нами,и которые своим творчеством прославляли то, что нас объединяет, кормит и дарит радость — родную землю.

Литературное краеведение может стать действительным помощником по воспитанию у молодежи любви к Родине, чувства красоты, познавательных интересов и способностей.

Литературное краеведение делает ближе к нам писателей и созданные ими произведения; способствует выработке активной жизненной позиции.

Литературное краеведение - это форма активного, действенного познания Родины, ее истории, ее культуры. **Нужно учиться понимать и любить жизнь, людей, землю, на которой родился.**

Список использованных источников

1. Аносова Л.Н. Писатели Белгородчины: библиографический указатель. / Л.Н. Аносова — Белгород, 1990. — С.73-77.
2. Литературная Белгородчина. 2020.URL: / http://literabel.ru/letbellibrary/vmikhalev.html (дата обращения 02.03.2021)
3. Токтарева А., Это классика. Что знаменитые писатели делали в Белгородской области. 2020.URL:https://www.belpressa.ru/society/drugoe/32059.html (дата обращения 27.03.2021)
4. Электронная библиотека – Википедия. 2020.URL: http://Wikipedia.ru(дата обращения 20.03.2021)

Направление 2

Информационно-телекоммуникационные технологии в науке и производстве

СЕКЦИЯ 2.1

НАУКА И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Алтынчурина Диана Ураловна, курсант 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Термин «технология» в переводе с греческого означает науку, совокупность способов и методов обработки или же переработки сырья, материалов, полуфабрикатов, изделий и переустройства их в предметы употребления. Современное осознание данного слова подключает и использование научных и инженерных познаний для заключения практической задачи. Информационно-телекоммуникационными технологиями можно считать те технологии, которые направлены на обработку и переустройства информации. Из вышесказанного следует, что информационно-телекоммуникационные технологии – это различные методы, способы и алгоритмы сбора, хранения, обработки, представления и передачи информации, то есть совокупность способов и средств передачи различной информации, материальную основу которых составляют наземные, спутниковые, сотовые и волоконно-оптические линии связи.

Информационные технологии призваны решать задачи по эффективной организации информационного процесса для снижения затрат времени, труда, энергии и материальных ресурсов во всех сферах человеческой деятельности, основываясь на внедрении современных достижений в области компьютерной техники и иных высоких технологий, новейших средств коммуникации, программного обеспечения и практического опыта. Информационные технологии нередко применяются в сфере услуг, области управления, промышленного производства, социальных процессов.

Информационные технологии охватывают все ресурсы, необходимые для управления информацией, особенно компьютеры, программное обеспечение и сети, которые важны для создания, хранения, управления, передачи и поиска информации. Информационные технологии могут быть разделены следующим образом:

- Технические средства;
- Коммуникационные средства;
- Организационно-методическое обеспечение;
- Стандартизация.

В современном мире с каждым днем возрастает роль компьютерных нововведений, различных программных средств. Информационные технологии используются во всех сферах деятельности, они явились итогом информационной инфраструктуры, которая связана с новым типом общественных отношений, с новой реальностью, с новыми информационными технологиями различных видов деятельности, они играют весомую роль в области образования, науки, производства и т. д. Так как любая наука — это прежде всего информация, то применение IT-технологий во всякой науке стало обязательной частью происходящих в мире процессов. Информационные технологии в науке и образовании способствуют автоматизации и эффективности учебно-познавательного процесса благодаря ускорению в обработке и передаче информации, реализации трудоемких задач.

Беспрерывно растущие в науке передовых информационно-телекоммуникационных технологий значимо расширяет способности ученных получать важную научную информацию. Полезности информационно-телекоммуникационных технологий ни разу не

вызывала колебаний для науки, но продуктивность не имела настоящих доказательств. В науке телекоммуникации играют особую роль, являясь не только необходимым условием индивидуальной научной деятельности, но и ее системообразующим механизмом. Через них труды отдельных ученных соединяются в научные области, направления и дисциплины. От эффективности и быстродействия научных телекоммуникаций зависит вся профессиональная деятельность научного сообщества.

Развитие компьютерных телекоммуникаций в российской науке началось с некоторым запозданием, вскоре стало предметом специального исследования. К началу 21 века широко распространялись информационно-телекоммуникационные технологии в отечественно научном сообществе и стали неотъемлемой частью профессиональной деятельности, многие из которых уже не представляли себе дальнейшей работы без использования этих технологий.

К сожалению, невозможно удовлетворить потребность ученых в информационно-телекоммуникационных технологиях, поэтому наши перспективы на хорошее место в мировой науке серьезнейшим образом связаны с тем насколько будет уделено время дальнейшему внедрению и развитию новейших сетевых информационно-телекоммуникационных технологий.

МЕЖСАЙТОВЫЙ СКРИПТИНГ КАК АКТУАЛЬНАЯ УГРОЗА СОВРЕМЕННЫХ ВЕБ-СИСТЕМ

Антропов Антон Владимирович, курсант 4-го курса
Научный руководительКазанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Обеспечение информационной безопасности в вычислительных системах является одной из главных задач, решаемых органами внутренних дел, в деятельности которой используются алгоритмы сбора, обработки, хранения, передачи информации. Большинство угроз информационной безопасности стали возможны благодаря широкому распространению сети Интернет. Развитие и рост Интернет-технологий оказывают как положительное, так и негативное влияние на правовую сферу в интернете. Согласное открытому проекту обеспечения безопасности веб-приложений (OWASP), XSS занимает 3 место в рейтинге среди ключевых рисков Web-приложений. По данным Всероссийского центра изучения общественного мнения 95,3 млн человек в России пользуются интернетом ежедневно. Пользователи сети Интернет активно используют веб-приложения, регистрируются на различных сайтах, предоставляют свои персональные данные владельцам данных ресурсов. Однако, защищенность ряда сайтов и баз данных от утечки информации о пользователях не всегда является надежной.

Популярность XSS атаки обусловлена простотой их реализации, минимальным набором инструментов для осуществления, а также невнимательностью разработчиков при создании веб-приложений. Принцип действия злоумышленника в данном случае основывается на том, что происходит внедрение вредоносного скрипта на стороне клиента в веб-страницу. Когда пользователь посещает веб-страницу, код скрипта загружается и прозрачно запускается веб-браузером. Одной из причин популярности уязвимостей XSS является то, что разработчики веб-приложений часто имеют мало или вообще не имеют опыта работы в области безопасности. Результатом является то, что плохо разработанный код, пронизанный недостатками безопасности, развертывается и становится доступным для всего интернета. В настоящее время XSS-атаки решаются путем устранения уязвимости на стороне сервера, которая обычно является результатом неправильных процедур проверки входных данных.

XSS как сетевая атака. XSS (англ. Cross-SiteScripting — «межсайтовый скриптинг») — тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницувредоносного кода (который будет выполнен на компьютерепользователя при открытии им этой страницы) и взаимодействии этого кода с веб-сервером злоумышленника. Межсайтовый скриптинг является разновидностью атаки «внедрение кода».

Межсайтовая скриптовая атака - это инъекция вредоносного кода, который будет выполняться в браузере жертвы. Вредоносный скрипт может быть сохранен на веб-сервере и выполняться каждый раз, когда пользователь вызывает соответствующую функциональность. Он также может быть выполнен другими методами – без какого-либо сохраненного скрипта на веб-сервере.

Основная цель этой атаки – украсть идентификационные данные другого пользователя - файлы cookie, токены сеанса и другую информацию. В большинстве случаев эта атака используется для кражи файлов cookie другого человека. Как мы знаем, файлы cookie помогают нам автоматически входить в систему. Поэтому с помощью украденных файлов cookie мы можем войти в систему с другими идентификаторами. И это одна из причин, почему эта атака считается одной из самых рискованных атак.

XSS-атака выполняется на стороне клиента. Он может быть выполнен с использованием различных клиентских языков программирования. Однако чаще всего эта атака выполняется с помощью Javascript и HTML.

С точки зрения злоумышленников особый интерес представляют две вещи: файлы cookie, связанные с документом, и учетные данные доступа. JavaScript также предоставляет возможности доступа к этой информации.Одной из причин популярности уязвимостей XSS является то, что разработчики веб-приложений имеют мало или вообще не имеют опыта работы в области безопасности.

Межсайтовый скриптинг является популярной атакой на веб-приложение. Подводя итог, хочется затронуть аспекты безопасности, существует множество защитных методов, включая следующие аспекты, для предотвращения XSS:

- статический анализ;
- динамический анализ;
- тестирование черного ящика;
- тестирование белого ящика;
- обнаружение аномалий.

Как правило, эти подходы развертываются на стороне клиента или сервера для защиты веб-пользователей от атаки XSS-инъекций.Также, необходимо не забывать об аспектах, которые помогают обезопасить веб-страницу от XSS, посредством проведения входной фильтрации и фильтрации вывода, кроме этого установив брандмауэр приложений, предотвращающий XSS-атаки.

ВИРУСЫ И ВРЕДОНОСНЫЕ ПРОГРАММЫ

Аушев Исраил Рустамович, курсант 1-го курса
Научный руководительОвчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Большинство вирусов и вредоносных компьютерных программ распространяются посредством зараженных файлов на файлообменниках, таких как одноранговые сети и торренты

Разработчики вредоносных программ часто пытаются обманом заставить пользователей скачивать вредоносные файлы. Это может быть письмо с вложенным файлом, который описывается как уведомление о доставке, возврат налогового платежа или счет по купленному билету. В письме может быть сказано, что необходимо открыть вложение, чтобы получить отправление или деньги.

Если вы откроете вложение, то на ваш компьютер будет установлена вредоносная программа.

Иногда вредоносное письмо легко заметить: в нем может быть орфографические и грамматические ошибки, или оно может быть отправлено с незнакомого электронного адреса. Тем не менее, эти письма могут выглядеть и так, будто их отправила настоящая компания или знакомый вам человек. Некоторые вредоносные программы могут взламывать учетные записи электронной почты и использовать их для отправки вредоносной нежелательной почты на все адреса, найденные в списке контактов.

Для защиты компьютера от заражения рекомендуется учесть следующее.

- Если вы не уверены, что знаете отправителя, или что-то кажется подозрительным, не открывайте письмо.
- Если в письме сказано, что вам нужно обновить ваши данные, не переходите по ссылке в письме.
- Не открывайте вложение в письме, которого вы не ждали или отправитель которого вам не известен.

Дополнительные сведения см. в статье Защита от фишинга.

В MicrosoftOneDrive встроена система защиты от атак программ-шантажистов. Дополнительные сведения см. в статье Обнаружение программы-шантажиста и восстановление файлов

РЕАЛИЗАЦИЯ ЗАЩИТЫ ОТ АТАКИ “БРУТФОРС”

Ахунов Александр Альфисович, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Брутфорс–это метод автоматизированного подбора пароля и логина путем грубого перебора. Данная атака основана на математическом методе bruteforce заключающемся в поиске решения исчерпыванием всех возможных вариантов. Программное обеспечение генерирует множество комбинаций при помощи которых злоумышленники получают доступ к конфиденциальной информации, документам для служебного пользования и прочему виду информации, которая не предназначена для огласки третьим лицам. Данная атака – это популярный метод для взлома учетных записей пользователей будь то каких-либо онлайн игр, почтовых сервисов, социальных сетей (вконтакте, facebook и тд.). Однако с развитием систем защиты, минимальным требованиям к паролю владельца учетной записи, эффективность брутфорса уменьшается.

Прежде всего,чтобы предотвратить успешную атаку грубой силы, необходимо уделить паролю должное внимание,например:

- Создавать криптоустойчивые пароли; они должны быть длиной не меньше 10-12 символов (но лучше 15-20 сим) и состоять из букв, цифр и спецсимволов. Например можно использовать какой-либо генератор паролей.10-символьные пароли, которые включают символы или цифры создают 171,3 квинтиллиона (1,71 x 10 20) возможностей. Используя процессор GPU , который пытается 10,3 миллиарда хэшей в секунду, взлом пароля займет примерно 526 лет, хотя суперкомпьютер может взломать его в течение нескольких недель.
- Не использовать в качестве пароля свой логин
- Не применять в качестве пароля информацию,которую можно узнать в сети интернет,например фамилию, имя, год рождения, номер телефона и тд.
- Не использовать одинаковые пароли для разных учетных записей
- Избегать популярных шаблонных паролей(см.ниже)

Пользователи имеют много учетных записей и имеют много паролей. Люди, как правило, неоднократно используют несколько простых паролей, что оставляет их открытыми для атак грубой силы. Кроме того, повторное использование одного и того же пароля может предоставить злоумышленникам доступ ко многим учетным записям.

Учетные записи электронной почты, защищенные слабыми паролями, могут быть подключены к дополнительным учетным записям, а также могут использоваться для восстановления паролей. Это делает их особенно ценными для хакеров. Кроме того, если пользователи не изменяют свой пароль маршрутизатора по умолчанию, их локальная сеть уязвима для атак. Злоумышленники могут попробовать несколько простых паролей по умолчанию и получить доступ ко всей сети.

Некоторые из наиболее часто встречающихся паролей в списках грубой силы включают: дату рождения, имена детей, qwerty, 123456, abcdef123, a123456, abc123, пароль, asdf, hello, welcome, zxcvbn, Qazwsx, 654321, 123321, 000000, 111111, 987654321, 1q2w3e, 123qwe, qwertyuiop, gfhjkm.

Надежные пароли обеспечивают лучшую защиту от кражи личных данных,потери данных, несанкционированного доступа к учетным записям и т.д.

Как администратор, есть методы, которые вы можете реализовать, чтобы защитить пользователей от взлома пароля грубой силой:

- Политика блокировки-возможность заблокировать учетные записи после нескольких неудачных попыток входа в систему, а затем разблокировать его от имени администратора.
- Прогрессивные задержки-возможность заблокировать учетные записи в течение ограниченного периода времени после неудачных попыток входа в систему. С каждой попыткой задержка увеличивается.
- Captcha-инструменты, такие как reCAPTCHA, требуют от пользователей выполнения простых задач для входа в систему. Пользователи могут легко выполнять эти задачи, в то время как инструменты грубой силы не могут.
- Требование надежных паролей- возможность заставить пользователей определять длинные и сложные пароли. Вы также должны применять периодические изменения пароля.
- Двухфакторная проверка подлинности-возможность использовать несколько факторов для проверки подлинности удостоверения и предоставления доступа к учетным записям.

Список использованных источников

1. Андреев Н.Н. О некоторых направлениях исследований в области защиты информации / Н.Н. Андреев // Международная конференция “Безопасность информации”. - 1997. - №2. - С. 94-97.

2. Баричев С.С. Основы современной криптографии / С.С. Баричев, В.В. Гончаров, Р.Е. Серов // - 1997. - №1

АНАЛИЗ УЯЗВИМОСТЕЙ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ

Байков Даниил Вадимович, командир отделения 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В современном мире подход к проектированию автоматизированной системы безопасности того или иного объекта, предполагает собой взаимное интегрирование различных подсистем безопасности, вне зависимости от того, когда идёт речь о крупном объекте или же об офисе, состоящем из нескольких кабинетов.

Рассмотрим функции и элементы системы безопасности.

Безопасность организации, компании, офиса, производственного или иного помещения обеспечивается целым комплексом мер. К важной составляющей выявления угроз и их нейтрализации относятся системы безопасности. Они нужны на любом коммерческом объекте. Системы безопасности обеспечивают стабильность работы организации, выполняя различные функции защиты и контроля.

Первоочередная задача любого комплекса – это охрана организации от внешних и внутренних угроз. В роли таких угроз, в основном, рассматривают следующее:

- перехват управления предприятием;
- подрыв деловой репутации компании;
- материальный ущерб;
- попытка хищения имущества или коммерческой тайны;
- возникновение пожара, аварии и других опасных для жизни и здоровья людей ситуаций.

Именно системы безопасности способны справиться с предупреждением подобных угроз, путем обеспечения контроля доступа на территорию предприятия и охраняемых объектов, мониторингом ситуации в режиме реального времени и принятием срочных мер в случае возникновения чрезвычайных ситуаций.

Основные системы безопасности

Для обеспечения полной безопасности в организациях устанавливаются системы контроля доступа и сканеры безопасности, системы сигнализации и видеонаблюдения, системы противопожарной защиты и т.д. Рассмотрим каждый тип наиболее распространенных систем более подробно.

1. Системы контроля доступа

Контроль доступа - это первое, о чем должно позаботиться любое предприятие. Независимо от величины вашего объекта, вы можете сократить расходы на обычную охрану, установив современную систему контроля доступа. Ограничивать доступ можно как в целом на объект, так и в отдельные его помещения (например, в сейфы), а также на парковки. Для этого, согласно ГОСТ Р 51241-2008, используются:

- Ограждающие устройства (шлагбаумы, турникеты, дорожные блокираторы, шлюзовые кабины и т.д.);
- Пропускная система или устройства ввода идентификационных признаков (в том числе - системы распознавания номеров автомобилей, управления передвижения транспортных средств и 3D-распознавание лиц);
- Устройство управления, защищенное от несанкционированного доступа. Система контроля доступа особенно необходима в финансовых организациях, банках, учебных и государственных учреждениях, на предприятиях, на режимных и военных объектах. Считывателями и преграждающими устройствами необходимо оборудовать главные и

служебные входы, КПП, помещения, в которых хранятся материальные ценности и где работает руководство.

В местах большого скопления людей также применяются сканирующие устройства, которые позволяют ускорить процесс досмотра большого количества людей на вокзалах, в аэропортах, в крупных торговых центрах, на массовых мероприятиях.

2. Системы видеонаблюдения

Системы видеонаблюдения или охранного телевидения позволяют следить за разными объектами и территориями. Видеонаблюдение эффективно при выполнении контролирующих функций в многоэтажных помещениях, административных зданиях, а также на больших производственных площадях. Кроме того, помогают отслеживать прилегающие территории. Главная задача таких систем - контроль ситуации. В случае получения тревоги именно видеонаблюдение позволяет определить характер и место нарушения и принять оптимальные меры.

В состав системы охранного телевидения, согласно ГОСТ Р 51558-2000, должны входить:

- камера видеонаблюдения;
- видеомонитор;
- источник электропитания;
- линии передачи.

3. Системы сигнализации

Охранная сигнализация.

Чаще всего, говоря о сигнализации, имеют в виду именно охранную сигнализацию, которая используется для защиты периметра территорий и открытых площадок, зданий, помещений, отдельных предметов. Защита периметра и помещений имеет некоторые свои отличительные особенности. Основными из них являются: оперативность обработки сигнала, автоматизированность системы.

Есть еще один вид охранной сигнализации - тревожная, которая активизируется при помощи человека, оказавшегося в ситуации угрозы. Такая «тревожная кнопка» обязательно должна быть в хранилищах, сейфах, в помещениях для хранения оружия и боеприпасов, в торговых точках и пунктах обмена валют на рабочих местах кассиров, в кабинете бухгалтера и руководителя, на постах охраны, у всех входов в здание.

4. Автоматическая пожарная сигнализация

Основная задача пожарной сигнализации - выявление возгорания и оповещение об опасности. Требования к обеспечению противопожарной безопасности объектов содержатся в Техническом регламенте о требованиях пожарной безопасности № 123-ФЗ и сводах правил к нему.

5. Системы оповещения при пожаре и системы пожаротушения

Главная задача любой системы оповещения - оперативно информировать людей о возникшей нештатной ситуации и осуществлять координацию их действий по выполнению эвакуации с опасного объекта. Это может быть подача звуковых и/или световых сигналов и трансляция речевой информации о характере опасности и путях эвакуации.

Очевидно, систем безопасности очень много и, используя различные её варианты, решаются важные для жизни, здоровья людей или защиты объекта задачи. Поэтому эффективнее всего использовать комплексный подход, когда проектированием, монтажом и обслуживанием всех систем занимается одна компания, обеспечивая целый комплекс мер.

Как уже было сказано, при организации системы безопасности и доступа эффективнее использовать именно комплексный подход. Важно организовать защиту и контроль на всех уровнях, и комплексный подход позволяет сделать это максимально успешно. К примеру, одни из основных преимуществ данного подхода:

- Оперативность. Комплексный подход позволяет добиться высокой скорости передачи данных даже в том случае, если разные системы защиты будут срабатывать одновременно. Моментальное реагирование - залог вашего спокойствия.

- Надежность. В основе комплексного подхода - грамотное проектирование и продуманность всех деталей. Вы не упустите ни одной важной составляющей. Из работы исключается человеческий фактор (усталость, невнимательность), поэтому такой подход обеспечивает высокий уровень надежности и защищенности.
- Интегрированность. Все системы безопасности при комплексном подходе связаны между собой. Таким образом создается интегрированная среда обмена сигналами между различными элементами. Все системы работают в комплексе, выполняя одновременно функции контроля, сдерживания, обнаружения опасности, ее оценки и реагирования на нее, обеспечивая защиту сразу по нескольким направлениям.

Важно понимать, что система безопасности необходима практически каждому современному предприятию. Грамотное проектирование таких систем позволяет реализовать целый ряд возможностей, не выходя за рамки отведенных бюджетов. Проект должен предусматривать возможное расширение площадей и введение в систему новых элементов.

Оценка уровня уязвимости каждой из системы, входящей в автоматизированную систему безопасности методом Саати

Для того, чтобы дать качественную оценку уровню эффективности той или иной автоматизированной системе безопасности, необходимо рассмотреть данный вопрос в контексте комплексного подхода. То есть как было сказано ранее, необходимо рассмотреть автоматизированную систему безопасности как совокупность основных систем безопасности, а именно:

1. Система контроля доступа;
2. Система видеонаблюдения;
3. Система сигнализации;
4. Автоматизированная противопожарная сигнализация;
5. Системы оповещения при пожаре и системы пожаротушения.

Подробное описание каждого из видов систем безопасности представлено было ранее, поэтому на данном этапе описания даваться не будет.

Описание показателей:

1) P_1: Система контроля доступа
2) P_2: Система видеонаблюдения
3) P_3: Система сигнализации
4) P_4: Автоматизированная противопожарная сигнализация
5) P_5: Системы оповещения при пожаре и пожаротушения

В связи с тем, что задача определения наиболее уязвимых компонентов комплексной безопасности объекта, при многообразии различных систем в одном помещении, является задачей достаточно трудоемкой, необходимо ввести взвешенный показатель, оценивающий различные системы по определенным параметрам.

Обозначим α_t - взвешенный показатель уязвимости компонентов комплексной системы безопасности объекта.

Так как α_t не поддается непосредственному измерению, его значение будет определяться экспертами методом попарных сравнений с использованием метода Саати.

Условимся, что следующие числа будут характеризовать сравнение уязвимость каждой из систем, входящих в автоматизированную систему безопасности в целом:

1 – P_t и P_s имеют одинаковую уязвимость;

3 – P_t незначительно уязвимее, чем P_s ;

5 – P_t значительно уязвимее, чем P_s ;

7 – P_t явно уязвимее, чем P_s ;

9 – P_t по своей уязвимости абсолютно превосходит P_s .

На основании определенных экспертами рангов строится матрица парных сравненийотносительной значимости признаков P^t с элементами $P_{ij}^t = \frac{P_i^t}{P_j^t}$, где t –индекс, характеризующий компоненту комплексной системы безопасности. Следующий шаг заключается в вычислении векторов приоритетов $V_{P^t} = (\alpha_1^t, ..., \alpha_5^t)$. Для примера рассмотрим вычисление вектора приоритетов, который представляет собой собственный вектор матрицы и может быть найден как решение уравнения:

$$P^t \cdot V_{P^t} = \lambda \cdot V_{P^t} \quad (1)$$

где λ – собственное значение матрицы P^t.

Как видно из формулы (1) для определения собственного вектора матрицы необходимо найти ее собственные значения λ. В рамках данной работы не будем приводить методику расчетов собственных значений и векторов матрицы, а сразу отразим результаты моделирования.

С учетом оценок построена матрица парных сравнений предпочтений экспертов (таблица 1).

Таблица 1. Матрица парных сравнений относительной значимости признаков P_t.

	P_1	P_2	P_3	P_4	P_5
P_1	1	1/2	1/3	1/5	1/6
P_2	2	1	1/5	1/5	1/6
P_3	3	3	1	1/4	1/5
P_4	5	5	4	1	1/4
P_5	6	6	5	4	1

Отсюда формула (1) принимает вид:

$$\begin{bmatrix} 1 & 1/2 & 1/3 & 1/5 & 1/6 \\ 2 & 1 & 1/5 & 1/5 & 1/6 \\ 3 & 3 & 1 & 1/4 & 1/5 \\ 5 & 5 & 4 & 1 & 1/4 \\ 6 & 6 & 5 & 4 & 1 \end{bmatrix} \times \begin{bmatrix} \alpha_1^t \\ \alpha_2^t \\ \alpha_3^t \\ \alpha_4^t \\ \alpha_5^t \end{bmatrix} = \lambda \times \begin{bmatrix} \alpha_1^t \\ \alpha_2^t \\ \alpha_3^t \\ \alpha_4^t \\ \alpha_5^t \end{bmatrix}$$

После проведенных расчетов были получены следующие значения значимости показателей $\alpha_t : \alpha_1 = 0.048,\ \alpha_2 = 0.064,\ \alpha_3 = 0.17,\ \alpha_4 = 0.261,\ \alpha_5 = 0.51.$ Анализируя полученные результаты нетрудно заметить, что показатель, характеризующий систему оповещения при пожаре и систему пожаротушения, явно отличается от всех остальных полученных показателей, причем, как минимум, в два раза. Всё это позволяет сделать вывод о том, что данный показатель является наиболее уязвимым, среди всех компонентов системы безопасности и нуждается в модернизации в первую очередь.

Разработанная модель оценки эффективности каждого из показателей методом Саати позволяет дать оценку уровня уязвимости каждой из компонент автоматизированной системы безопасности. Полученная информация будет полезна при анализе уровня безопасности и оценки необходимости модернизации той или иной системы безопасности, с целью устранения недостатков в ней, повышающих уязвимость объекта. Также данным

методом удобно пользоваться при выборе наиболее подходящего оборудования для конкретного объекта защиты.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Баранова Анастасия Андреевна, курсант 903 учебного взвода
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1.Конфиденциальность. Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.

2.Целостность. Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.

3.Доступность. Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Контроль информационной безопасности

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней. Выделяют следующие виды контроля:

1. Административный. Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.

2. Логический. Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам, программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

3. Физический. Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Угрозы информационной безопасности

Угрозы информационной безопасности можно разделить на следующие:

Естественные (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).

Искусственные, которые также делятся на:

- непреднамеренные (совершаются людьми по неосторожности или незнанию);
- преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).

Внутренние (источники угрозы, которые находятся внутри системы).

Внешние (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например применение специальных программ).

Средства защиты информационной безопасности

Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.

Средства защиты информации делятся на:

Организационные. Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и организационно-правовых (законодательная база, статут конкретной организации) средств.

Программные. Те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.

Технические (аппаратные). Это технические виды устройств, которые защищают информацию от проникновения и утечки.

Смешанные аппаратно-программные. Выполняют функции как аппаратных, так и программных средств.

ЗАЩИТА ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

Баринова Анастасия Константиновна, курсант 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Исторически первый и наиболее распространенный вид работы в телекоммуникационных сетях - межперсональный обмен текстовыми сообщениями, известный под названием «электронная почта» (или E-mail). Как и при обычной почтовой связи, здесь происходит обмен сообщениями, но не на бумаге, а в виде файлов. Преимущества электронной почты над обычной велики: многократно большая скорость доставки информации (так, сообщение из России в США обычно доставляется не более, чем за 2 часа), компьютерная подготовка сообщений, передача информации в виде, допускающем последующую ее компьютерную обработку получателем (редактирование, помещение в различные документы, базы данных и т.д.).

Пользователь все больше хочет быть уверен, что отправленные им сообщения никто не прочитает, кроме указанного адресата. Получатель же хочет быть уверен, что информация получена именно из того источника, от которого он их ожидал. Для решения целей обеспечения безопасности передаваемой информации во всем мире все активнее применяются технологии криптографической защиты с использованием открытых ключей.

По мере расширения использования систем электронной почты в российском деловом мире стремительно растет и количество конфиденциальных данных, передаваемых по сети Интернет. В результате становится актуальной проблема автоматизации и защиты документооборота, осуществляемого с помощью средств электронной почты: хочется быть уверенным, что отправленные сообщения никто не прочитает, кроме указанного адресата. Важно также быть уверенным, что отправляемые электронные документы в процессе пересылки и хранения не будут подделаны.

Угрозы, связанные с электронной почтой

Основные протоколы передачи почты (SMTP, POP3, IMAP4) обычно не осуществляют надёжной аутентификации, что позволяет легко создать письма с фальшивыми адресами. Ни один из этих протоколов не использует криптографию, которая могла бы гарантировать конфиденциальность электронных писем. Хотя существуют расширения этих протоколов, решение использовать их должно быть явно принято как составная часть политики администрации почтового сервера. Некоторые такие расширения используют уже имеющиеся средства аутентификации, а другие позволяют клиенту и серверу согласовать тип аутентификации, который будет использоваться в данном соединении.

1. Фальшивые адреса отправителя

Адресу отправителя в электронной почте Интернета нельзя доверять, так как отправитель может указать фальшивый обратный адрес, или заголовок может быть модифицирован в ходе передачи письма, или отправитель может сам соединиться с SMTP-портом на машине, от имени которой он хочет отправить письмо, и ввести текст письма.

2. Перехват письма

Заголовки и содержимое электронных писем передаются в чистом виде. В результате содержимое сообщения может быть прочитано или изменено в процессе передачи его по Интернету. Заголовок может быть модифицирован, чтобы скрыть или изменить отправителя, или для того чтобы перенаправить сообщение.

3. Почтовые бомбы

Почтовая бомба - это атака с помощью электронной почты. Атакуемая система переполняется письмами до тех пор, пока она не выйдет из строя. Как это может случиться, зависит от типа почтового сервера и того, как он сконфигурирован.

Некоторые провайдеры Интернета дают временные логины любому для тестирования подключения к Интернету, и эти логины могут быть использованы для начала подобных атак.

Типовые варианты выхода почтового сервера из строя:

- Почтовые сообщения принимаются до тех пор, пока диск, где они размещаются, не переполнится. Следующие письма не принимаются. Если этот диск также основной системный диск, то вся система может аварийно завершиться.

- Входная очередь переполняется сообщениями, которые нужно обработать и передать дальше, до тех пор, пока не будет достигнут предельный размер очереди. Последующие сообщения не попадут в очередь.

- У некоторых почтовых систем можно установить максимальное число почтовых сообщений или максимальный общий размер сообщений, которые пользователь может принять за один раз. Последующие сообщения будут отвергнуты или уничтожены.

- Может быть превышена квота диска для данного пользователя. Это помешает принять последующие письма, и может помешать ему выполнять другие действия. Восстановление может оказаться трудным для пользователя, так как ему может понадобиться дополнительное дисковое пространство для удаления писем.

- Большой размер почтового ящика может сделать трудным для системного администратора получение системных предупреждений и сообщений об ошибках .

- Посылка почтовых бомб в список рассылки может привести к тому, что его члены могут отписаться от списка.

Способы защиты электронной почты

1. Защита от фальшивых адресов

От этого можно защититься с помощью использования шифрования для присоединения к письмам электронных подписей. Одним популярным методом является использование шифрования с открытыми ключами. Однонаправленная хэш-функция письма шифруется, используя секретный ключ отправителя. Получатель использует открытый ключ отправителя для расшифровки хэш-функции и сравнивает его с хэш-функцией, рассчитанной по полученному сообщению. Это гарантирует, что сообщение на самом деле написано отправителем, и не было изменено в пути. Правительство США требует использования алгоритма SecureHashAlgorithm (SHA) и DigitalSignatureStandard, там, где это возможно. А самые популярные коммерческие программы используют алгоритмы RC2, RC4, или RC5 фирмы RSA.

2. Защита от перехвата

От него можно защититься с помощью шифрования содержимого сообщения или канала, по которому он передается. Если канал связи зашифрован, то системные администраторы на обоих его концах все-таки могут читать или изменять сообщения. Было предложено много различных схем шифрования электронной почты, но ни одна из них не стала массовой. Одним из самых популярных приложений является PGP. В прошлом использование PGP было проблематичным, так как в ней использовалось шифрование, подпадавшее под запрет на экспорт из США. Коммерческая версия PGP включает в себя плагины для нескольких популярных почтовых программ, что делает ее особенно удобной для включения в письмо электронной подписи и шифрования письма клиентом. Последние версии PGP используют лицензированную версию алгоритма шифрования с открытыми ключами RSA.

Корректное использование электронной почты

Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что, когда письмо посылается, как отправитель, так и получатель должен гарантировать, что взаимодействие между ними

осуществляется согласно принятым правилам взаимодействия. Взаимодействие с помощью почты не должно быть неэтичным, не должно восприниматься как конфликтная ситуация, или содержать конфиденциальную информацию.

Политика защиты электронных писем и почтовых систем.

Защита писем, почтовых серверов и программ должна соответствовать важности информации, передаваемой по сетям. Как правило, должно осуществляться централизованное управление сервисами электронной почты. Должна быть разработана политика, в которой указывался бы нужный уровень защиты.

Заключение

Все служащие должны использовать электронную почту так же, как и любое другое официальное средство организации. Из этого следует, что когда письмо посылается, как отправитель, так и получатель должен гарантировать, что взаимодействие между ними осуществляется согласно принятым правилам взаимодействия.

Как правило, должно осуществляться централизованное управление сервисами электронной почты. Должна быть разработана политика, в которой указывался бы нужный уровень защиты.

ФОРМИРОВАНИЕ ЦИФРОВОЙ КОМПЕТЕНТНОСТИ У СОТРУДНИКОВ ПОЛИЦИИ

Белов Ярослав Михайлович, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Состояние современного мира стремительно изменилось за последние годы, и народы, населяющие планету, перешли от «индустриального общества» к «обществу информационному». Произошла смена способов производства, мировоззрения людей, их образа жизни

Информационные технологии кардинальным образом поменяли жизнь миллионов людей. Информация стала важнейшим стратегическим, управленческим ресурсом наряду с ресурсами — человеческим, финансовым, материальным. Производство и потребление информации составляют необходимую основу эффективного функционирования и развития различных сфер экономики и общественной жизни, и напрямую влияют на жизнь государств и народов

Стратегия развития информационного общества в Российской Федерации на 2017—2030 годы предполагает формирование в России цифровой экономики. В целях развития информационного общества государством создаются условия для формирования пространства знаний и предоставления доступа к нему, совершенствования механизмов распространения знаний, их применения на практике в интересах личности, общества и государства.

Федеральный закон «О полиции» от 7 февраля 2011 г. N 3-ФЗ провозгласил использование достижений науки и техники, современных технологий и информационных систем основным ПРИНЦИПОМ ДЕЯТЕЛЬНОСТИ ПОЛИЦИИ, законодательно закрепив инновационные процессы в правоохранительной сфере, и стимулировал внедрение инновационных продуктов мира цифровых технологий в деятельность органов внутренних дел, положив основу создания единой системы информационно-аналитического обеспечения деятельности МВД России (ИСОД МВД России), которая интегрировала в себя используемые в МВД России автоматизированные системы обработки информации, программно-аппаратные комплексы и комплексы программно-технических средств, системы связи и передачи данных, необходимые для эффективного обеспечения оперативно-служебной и служебно-боевой деятельности.

Информатизация и частичная автоматизация процессов проникла во все сферы деятельности полиции: начиная от оперативных подразделений и заканчивая тыловой службой, юридическими и кадровыми подразделениями.

В современной мировой педагогике просматриваются основные направления развития профессиональных навыков, которые подходят и к подготовке современного специалиста-полицейского.

HardSkills — так называемые «жёсткие навыки». Это совокупность профессиональных навыков, необходимых для чёткого и правильного выполнения работы, их можно проверить с помощью тестов и экзаменов. В случае полицейского — это знание нормативно-правовой базы, владение приёмами борьбы, оружием, умение документировать преступную деятельность и многое другое.

SoftSkills — «мягкие навыки», их нельзя проверить в тестовой форме. Это совокупность особых навыков, необходимые людям для общения, помогающие человеку не только в карьерном росте, но и в обычной жизни. Полицейскому необходимо умение работать в команде, общаться с гражданами, иметь способность регулировать своё

эмоциональное состояние. Это направление часто называют как «эмоциональный интеллект» и «социальный интеллект».

Digital — цифровая компетентность: основанная на непрерывном овладении компетенциями (системой соответствующих знаний, умений, мотивации и ответственности), способность индивида уверенно, эффективно, критично и безопасно выбирать и применять инфокоммуникационные технологии в разных сферах жизнедеятельности (информационная среда, коммуникации, потребление, техносфера), а также его готовность к такой деятельности.

Формирование цифровой компетентности — это одно из основных требований современного образования полицейского. Появляются новые формы информационного обеспечения деятельности полиции, которые, в некоторых случаях, дают возможность раскрывать преступления, не выходя из стен служебного кабинета.

Каждый современный полицейский должен уметь:

- пользоваться электронным документооборотом (с использованием цифровой подписи);
- пользоваться служебной почтой;
- использовать базы данных и информационные ресурсы органов внутренних дел и других государственных органов;
- использовать цифровые технологии в своей служебной деятельности в зависимости от специализации (например, эксперт);
- иметь навыки в области информационной безопасности и защиты информации.

Всё это диктует новые требования к подготовке современного полицейского: формирование цифровой компетентности наряду с базовыми юридическими знаниями и другими традиционными для юридического вуза МВД направлениями подготовки.

На наш взгляд, формирование цифровой компетентности современного полицейского должно охватывать, по крайней мере, три направления: цифровые навыки для обеспечения повседневной деятельности; навыки работы с информацией ограниченного доступа в цифровом виде (обеспечение информационной безопасности ОВД) и специальные навыки, позволяющие бороться с преступностью, используя информационные технологии.

Московский университет МВД России имени В.Я. Кикотя уже много лет, опережая время, готовит полицейских, владеющих современными информационными технологиями. Несколько лет назад появление таких специалистов было инновацией.Ежегодно факультет подготовки специалистов в области информационной безопасности выпускает специалистов, обладающих в полной мере «цифровой компетентностью», которые востребованы заказчиками кадров, такими как: подразделения оперативно-разыскной информации, подразделения связи, информационных технологий и защиты информации; подразделения специальных технических мероприятий. Обучение проводится в соответствии со специальностью 10.05.05. Безопасность информационных технологий в правоохранительной сфере по специализациям: технологии защиты информации в правоохранительной сфере; информационно-аналитическое обеспечение правоохранительной деятельности; компьютерная экспертиза при расследовании преступлений; (в перспективе: оперативно-техническое обеспечение раскрытия и расследования киберпреступлений в финансово-кредитной сфере, набор 2017 г.).

За последние два года произошло переоснащение лабораторной базы факультета, переработка тематических планов дисциплин. Налажены связи с практическими органами, сотрудники которых являются постоянными гостями и участниками образовательного процесса.

Изменён порядок организации и проведения итогового государственного экзамена, который впервые в этом году проходил в виде выполнения практической задачи, в ходе решения которой выпускник должен продемонстрировать полученные знания, умения, навыки и готовность к выполнению служебных обязанностей.

Новым вызовом времени является активизация киберпреступности, в особенности в банковской сфере. В течение последнего года в Московском университете МВД России развернулась активная работа по поиску решений в области подготовки полицейских кадров, способных принять вызов киберпреступности. Идёт интенсивная переработка учебных программ, методик преподавания, поиск новых решений в области углубления и расширения горизонтов цифровой компетентности полицейских кадров Российской Федерации.

Задача учебного заведения по формированию цифровой компетентности — дать представления курсантам и слушателям о возможностях современных технологий, знакомить с новинками в цифровом мире, формировать навыки работы на современном программном обеспечении, которые они потом смогут применить на практике.

В целях борьбы с преступностью необходимо знакомить курсантов и слушателей и с теми способами преступной деятельности, которые используют «продвинутые» представители преступного мира. Возросшая цифровая компетентность населения порождает и новые темпы роста преступлений, совершаемых с помощью информационных технологий. Количество киберпреступлений растёт, способы их совершения развиваются, становятся более профессиональными, вследствие чего несут угрозы не только гражданам и юридическим лицам, но также опасны для отдельных государств и для мирового сообщества в целом. В практику работы правоохранительных органов необходимо внедрять возможности сети Интернет и других высоких компьютерных технологий не только по выявлению и расследованию преступлений, но и по координации их деятельности. Для обеспечения таких дисциплин требуются специальные научные исследования по криминологии, криминалистике, праву, которые идут на стыке с изучением цифровых технологий.

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества. Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации. Для профессиональной подготовки современного специалиста формирование цифровой компетентности — необходимая часть знаний, умений и навыков, преподаваемых в любом высшем учебном заведении, идущем в ногу со временем. Не за горами то будущее, когда в нормативы профессиональной подготовки полицейского добавят упражнения по «цифровой компетентности».

Список использованных источников

1. Указ Президента РФ от 21.12.2016 N 699 (ред. от 25.12.2019) "Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации";
2. Приказ МВД России от 31 декабря 2019 г. N 995 "Об утверждении Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом (загранаппарате Министерства внутренних дел Российской Федерации)"
3. Федеральный закон "О полиции" от 07.02.2011 N 3-ФЗ
4. Указ Президента РФ от 01.03.2011 N 248 (ред. от 13.07.2020) "Вопросы Министерства внутренних дел Российской Федерации" (вместе с "Положением о Министерстве внутренних дел Российской Федерации")
5. Указ Президента РФ от 11.07.2004 N 865 (ред. от 17.09.2020) "Вопросы Министерства иностранных дел Российской Федерации"
6. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)

7. Глава 2 Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом: приложение к приказу МВД России от 31.12.2019 № 995
8. Федеральный закон "О полиции" от 07.02.2011 N 3-ФЗ (последняя редакция)
9. https://elibrary.ru/
10. https://xn--b1aew.xn--p1ai/
11. https://www.mid.ru/ru/home
12. https://books.google.ru/

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ОБЖИГОВОЙ МАШИНЫ АО «ЛГОК»

Белоус Артём Юрьевич, студент 4-го курса
Научный руководитель Хархота Надежда Васильевна, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Обжиговая конвейерная машина предназначена для сушки, подогрева, упрочняющего окислительного обжига и охлаждения железорудных окатышей. Процесс тепловой обработки окатышей на конвейерной машине заключается в постепенном их нагреве до температуры 1350 °С и последующем охлаждении.

Для этого сырые окатыши, уложенные на колосниковые решетки тележек с помощью укладчика и роликового питателя, последовательно проходят зоны сушки, подогрева, высокотемпературного обжига и рекуперации, охлаждения. Суммарное время пребывания окатышей на ленте машины составляет 20 – 30 мин.[1]

Целью исследования является расширенный анализ АСУ обжиговой машины ФОК АО «ЛГОК».

Задачи исследования:

- изучить характеристику технологического процесса обжиговой машины;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является обжиговая машина ФОК АО «ЛГОК».

Предмет исследования автоматизированная система управления обжиговой машины ФОК АО «ЛГОК».

Обжиговая конвейерная машина предназначена для сушки, подогрева, упрочняющего окислительного обжига и охлаждения железорудных окатышей. Процесс тепловой обработки окатышей на конвейерной машине заключается в постепенном их нагреве до температуры 1350 °С и последующем охлаждении.

Для этого сырые окатыши, уложенные на колосниковые решетки тележек с помощью укладчика и роликового питателя, последовательно проходят зоны сушки, подогрева, высокотемпературного обжига и рекуперации, охлаждения. Суммарное время пребывания окатышей на ленте машины составляет 20 – 30 мин. На ленту сначала укладывается донная и бортовая постели. Обжиг окатышей производится продуктами сгорания газа, сжигаемого при помощи горелок, устанавливаемых в укрытиях – камерах зон подогрева и обжига.

Обжиговая машины состоит из зон сушки, подогрева, обжига, рекуперации и охлаждения. В процессе термообработки окатыши перемещаются последовательно по всем зонам. Через обжиговую машину проходит сеть взаимосвязанных газоходов с переточными коллекторами, которые предназначены для транспортирования воздуха и продуктов сгорания по зонам. Прямой нагрев теплоносителя теплом от сжигания природного газа производится только в зоне обжига, в остальных же зонах для нужд технологического процесса используются вторичные источники тепла. В секциях зоны сушки и подогрева такими источниками тепла служат продукты сгорания и нагретый воздух, а в зонах охлаждения - охлаждающийся слой окатышей. Использование вторичных источников позволяет увеличить температуру слоя окатышей и воздуха на входе зоны обжига, что способствует снижению затрат природного газа.[3]

Определение режима термообработки, в котором удельный расход природного газа на обжиг окатышей минимален при соблюдении требований технологического регламента, осложняется следующими факторами:

- отсутствие возможности непосредственного контроля параметров слоя в зонах машины (температура, влажность);

- действия возмущений, обусловленных изменениями среднего диаметра гранул окатышей, скорости движения паллет ОМ, средней влажности и теплофизических свойств окатышей, а также порозности слоя.

Эти факторы вынуждают эксплуатационный персонал вести термообработку по косвенным параметрам (температура теплоносителя в зонах), поддерживая режим при котором температура слоя окатышей в зонах ОМ находится в окрестностях середины регламентного диапазона. Такой режим обжига позволяет свести к минимуму опасность выхода температуры окатышей под действием возмущений за пределы регламента, но далеко не всегда обеспечивает минимальные затраты природного газа.

Нижний уровень системы состоит из датчиков и исполнительных механизмов. Ультразвуковой датчик уровня Эхо-5 излучает ультразвуковую волну с периодически меняющейся частотой в направлении поверхности контролируемой среды.

Средний уровень системы состоит из шести микропроцессорных регулирующих контроллеров «Ремиконт Р-110» и одного кольца из четырёх контроллеров «Ремиконт Р-110»со шлюзом для осуществления обмена информацией с верхним уровнем системы (контроллером/сервером ввода-вывода). Микропроцессорными контроллерами Р-110 и Р-130 осуществляется сбор информации с датчиков измерения (преобразования), а также автоматическое регулирование контурами технологического процесса.

Верхний уровень системы состоит из трёх персональных ЭВМ офисного типа. Одна из ЭВМ служит контроллером/сервером ввода-вывода (в дальнейшем К/СВВ). Через К/СВВ осуществляется обмен информацией с микропроцессорными контроллерами Р-110 и Р-130, посредством установленного в К/СВВ 8-ми канального мультипорта «С168Р» фирмы Моха.

В результате анализа существующего уровня автоматизации были выявлены следующие недостатки:

- ненадежность работы контроллера «Ремиконт Р-130» (частые зависания, потеря данных и как следствие, нарушение технологического процесса);

- сложность интеграции контроллера «Ремиконт Р-130» в общую внутризаводскую сеть, система автоматического управления технологическим процессом выполнена с применением локальных контуров регулирования на базе контроллеров «Ремиконт Р-130».

Существующая система автоматического управления технологическим процессом является морально устаревшей, и не обеспечивает в полном объеме информацией о работе технологического оборудования ни персонал, ни обслуживающий это оборудование ни руководство комбината и фабрики, а также не может обеспечить автоматизированный сбор, регистрацию и отображение в реальном масштабе времени всех технологических значений, архивацию данных, хранение и дальнейшую передачу их в сеть ФОК и т.д.

Существующие контуры регулирования, реализуемые на Р-130, не обеспечивают необходимую точность стабилизации воздуха из-за сравнительно невысокого быстродействия контроллеров.

Датчик уровня не предоставляет точные данные о высоте слоя окатышей на транспортировочной ленте, т.к имеет большую погрешность и не способен охватить всю площадь измеряемой поверхности.

Автоматизированная система управления должна обеспечивать рациональное использование энергоресурсов, поддержание высокопроизводительной работы технологического оборудования, оптимизацию технологических параметров, безопасность технологического процесса.[2]

Предлагается провести модернизацию системы автоматизации обжиговой машины, а именно:

- заменить контроллер Ремиконт Р-130 на SIMATIC S7-1500;

- заменить датчики для измерения уровня слоя окатышей.

Программируемые логические контроллер Simatic S7-1500 с CPU 1510SP F-1 PN - это новейшее семейство контроллеров Сименс обладающих великолепными характеристиками, отличным набором функций и впечатляющим быстродействием. В новых контроллерах S7-1500 значительно снижено время реакции на внешние события.

Удобная конструкция программируемого контроллера S7-1500 и его модульность позволяют его максимально адаптировать к требованиям решаемой задачи. Контроллер имеет естественное охлаждение. В случае модернизации системы контроллер обеспечивает свободное наращивание функциональных возможностей. Повышенная степень защиты программы и данных обеспечивает дополнительный уровень безопасности.

Модернизация автоматической системы управления АСУ обжиговой машины ФОК АО «ЛГОК» заключается в экономии ресурсов производства и повышении надежности системы управлении.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. — 2-е изд. — Саратов : Ай Пи Эр Медиа, 2019. — 459 c. — ISBN 978-5-4486-0574-1. — Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83341.html. — Режим доступа: для авторизир. пользователей

КРИПТОГРАФИЯ В РУКАХ ПРЕСТУПНИКОВ

Бельдеубаева Даяна Ренатовна, курсант 4-го курса
Научный руководитель Поликарпов Евгений Сергеевич, начальник кафедры СИТ УНК ИТ, кандидат технических наук, подполковник полиции
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Рост киберпреступности в последние годы был поистине ошеломляющим. Международными экспертами по кибербезопасности Cybersecurity Ventures подсчитано, что в 2019 году в мире кибератаки происходят каждые 14 секунд. С увеличением числа кибератак возрастает и причиняемый ими ущерб. С 2015 год по 2018 год убытки в среднем возрастали на1-1,5 трлн долларовежегодно, в 2019 году они достигли уже 3трлн долларов. Cybersecurity Ventures прогнозирует, что ущерб от киберпреступности будет стоить миру $6 трлн. ежегодно к 2021году – это в несколько раз больше, чем ущерб, нанесенный стихийными бедствиями в год, и прибыльнее, чем глобальная торговля незаконными наркотиками. В России динамика роста преступлений в сфере информационных технологий за прошедшие три года составила 165 процентов. Каждое седьмое преступление совершается с помощью IT-технологий. По информации МВД, в 2019 году было зарегистрировано 294,4 тысячи преступлений, совершенных с использованием информационно-телекоммуникационных технологий, а в январе 2020 года правоохранительными органами РФ зарегистрировано 28,14 тысячи (+75,2%) преступлений. Только 5% киберпреступников были пойманы и осуждены за свои преступления, что свидетельствует о том, насколько сложно правоохранительным органам арестовывать и преследовать этих преступников.[1]

На основе вышеприведенных статистик можно сделать безоговорочный вывод о том, что киберпреступность является одной из самых больших и приоритетных проблем, с которыми столкнулось человечество. Она является самой быстрорастущей преступностью в мире. Последствия от киберпреступности включают в себя повреждение и уничтожение данных, кражу денег, потерю производительности, кражу интеллектуальной собственности, кражу личных и финансовых данных, хищение, мошенничество, нарушение нормального хода бизнеса после атаки, восстановление и удаление взломанных данных и систем, а также ущерб репутации.

Киберпреступность имеет относительно низкие риски по сравнению с другими видами преступной деятельности, и преступники осознали, что они могут заработать больше денег, с меньшим риском быть пойманными, прячась за программным обеспечением, которое скрывает их личность.

Прежде чем поймать преступника необходимо установить его личность и местоположение, для этого достаточно использовать сервер, который точно определит операционную систему клиентского компьютера, используемый браузер, время запроса и IP-адрес сервера провайдера Интернета и многое другое. Но не всё так легко, как, казалось бы, тут возникает проблема, потому что киберпреступники прежде всего заботятся о своей анонимности и безопасности и не хотят делиться реальным IP-адресом, через который их можно вычислить, а используют различные криптостойкие программные обеспечения для скрытия личных данных, такие как VPN, Tor, I2P, криптоконтейнеры, анонимные ОС, криптовалюты. Данные ПО, основанные на криптографической защите данных (шифровании), позволяют преступникам в процессе совершения киберпреступлений, обходить запреты того или иного государства, заметать следы и обеспечивать свою анонимность, безопасность, секретность личных данных. [2]

1. Зашифрованные и анонимные ОС

TailsOS - дистрибутив Linux на основе Debian, совокупность инструментальных средств для обеспечения анонимности и приватности. Все исходящие соединения проходят через сеть Tor, а все не анонимные блокируются. По завершению сессии невозможно определить действия злоумышленника на компьютере, даже получив доступ ко всему устройству, так как вся система работает в Live режиме и выгружается в оперативную память, а не на SSD или HDD. Данная ОС не предназначена для установки на жесткий диск в качестве постоянной операционной системы. Выключение или перезагрузка системы автоматически приводит к удалению всех скачанных файлов, истории браузера и т.д.Злоумышленники чаще всего используют Tails для быстрого доступа к удаленному web-ресурсу, связи по зашифрованному каналу и проведения некоторых криптовалютных операций.

Например, через Tails можно создать криптовалютный кошелёк с сохранением всех его данных в Persistent и при необходимости быстро перекинуть валюту, подключив флешку в любое устройство с интернетом.

Whonix OS - дистрибутив Linux на основе Debian, обеспечивающий высокую степень анонимности и безопасности средствами VirtualBox и Tor. Данная операционная система является достаточно устойчивой к проникновению вредоносных программ и минимизирует риск утечки IP-адреса и DNS. Программное обеспечение системы настроено с учётом всех требований безопасности. Whonix состоит из двух виртуальных машин, соединённых через изолированную сеть, Whonix-Gateway, которая работает только через Tor в качестве шлюза в сеть, и Whonix-Workstation, которая находится в полностью изолированной сети. В данном случае все сетевые соединения возможны только посредством Tor. Отличительной особенностью Whonix от других анонимных ОС является возможность модификации и детальной настройки. Whonix спасает хакеров от широко используемой спецслужбами деанонимизации, заключающейся в отправке файла с ID, который при открытии соединяется с сервером и незаметно передает данные об IP-адресе преступника в обход сети Tor. Ведь спасти от этого может только полная блокировка всех интернет-соединений и в таком случае файл не сможет ничего отправить.

LinuxKodachi OS - дистрибутив Linux на основе Debian, является контркриминалистической (anti-forensic) разработкой, учитывающей все особенности и тонкости процесса анонимности и безопасности, а также защиту самой системы. В Kodachi весь трафик автоматически проходит через преднастроенный VPN, затем через сеть Tor с DNS шифрованием. Kodachi затрудняет криминалистический анализ накопителей и оперативной памяти. Данная ОС более продумана, чем остальные анонимные ОС Linux. В Kodachi интегрирована поддержка DNScrypt -это протокол и одноименная утилита, шифрующая запросы к серверам OpenDNS методами эллиптической криптографии. Kodachi имеет огромное количество предустановленного софта для решения любых задач, например, для быстрого изменения выходных узлов с опцией выбора конкретной страны («MultiTor»),для шифрования информации (TrueCrypt, VeraCrypt), для передачи конфиденциальных сообщений (GnuPG, Enigmail, Seahorse, GNU Privacy Guard Assistant), для заметания следов (MAT, NepomukCleaner, Nautilus-wipe, BleachBit). Данный инструмент предоставляет идеальную возможность злоумышленникам воспользоваться огромным количеством программ для безопасного/анонимного доступа к сети, устанавливать связь по зашифрованным каналам через разные программы, замести все следы и тотально зашифровать всё необходимое.

2. VPN

Обычные сети из прокси-серверов больше не могут гарантировать полную анонимность и безопасность и защитить злоумышленника от специальных служб, так как весь трафик в открытом виде проходит через прокси-сервер третьих лиц. На смену прокси давно пришли виртуальные частные сети (virtual private networks) или VPN, которые являются широко известным способом туннелирования. VPN обеспечивает не только изолированный доступ к сети через цепочки VPN-серверов, но и шифрование передаваемых

данных. Тем самым данная технология позволяет обеспечить дополнительный уровень безопасности, получить доступ к контенту, запрещенному в стране проживания, скрыть трафик от интернет-сервис провайдера, а также скрыть местоположение и веб-предпочтения от остального мира.

Гибкость и анонимность, которые предоставляют подобные VPN-сервисы, делают их отличным инструментом для хакеров, которые не хотят оставлять свои следы, потенциально способные раскрыть их личность. Но как правило выбор VPN начинается с выбора протокола туннелирования. На данный момент широко используются следующие протоколы VPN: PPTP, L2TP, OpenVPN, SSTP. Среди них протокол OpenVPN по признанию большинства специалистов является лучшим и усовершенствованным. OpenVPN использует два канала: канал управления (control channel) и канал данных (data channel). В первом случае задействуется TLS - с его помощью ведется аутентификация и обмен ключами для симметричного шифрования. Эти ключи используются в канале данных, где и происходит само шифрование трафика. Преимуществами данного протокола являются - использование 256-битных ключей шифрования (OpenSSL-шифрование) и шифров высокого уровня (шифры AES, Camellia, 3DES, CAST-128 или Blowfish.); возможность с лёгкостью обойти любой фаервол на своем пути; работа как с TCP, так и с UDP, благодаря чему осуществляется больше контроля над соединениями; работа на значительно большем количестве платформ.

Также стоит отметить, что для предотвращения деанонимизации пользователя VPN, защиты от попыток спецслужб установить IP-адрес преступника «по ту сторону VPN», злоумышленниками используется цепочки VPN-серверов. Такие как DoubleVPN - цепь из двух VPN серверов, Triple VPN - из трех, Quadro VPN – из четырех. Пользователь подключается по шифрованному соединению к VPN серверу A, сервер A в свою очередь подключается по защищенному соединению с VPN к серверу B, а тот уже выходит в интернет.Таким образом, показатель защищенности информации, а это определяющая составляющая подключения, увеличивается в несколько раз.

3. Stunnel

Данную утилиту используют для обеспечения защищенного и зашифрованного соединения между удаленными клиентом и сервером посредством TLS и SSL без каких-либо изменений в коде программ, в случае если клиент и сервер не поддерживают данные протоколы самостоятельно. Для криптографии Stunnel использует библиотеку OpenSSL. Например, можно туннелировать трафик для netcat,vnc и даже bash.

Также данный инструмент шифрования может использоваться для маскировки трафика OpenVPN под «чистый» TLS, чтобы его было невозможно определить посредством DPI и, следовательно, заблокировать. Таким образом, получается схема: шифрование stunnel+ шифрование канала данных OpenVPN. Этот вариант позволит использовать RSA вместе с ECDSA.

4. OpenSSH

Это свободная реализация сетевого протокола, позволяющего создавать защищенные соединения, удаленно управлять операционной системой, туннелировать TCP-соединения (например, для передачи файлов). OpenSSH содержит: ssh - для замены rlogin и telnet, scp - для замены rcp и sftp - для замены ftp. Основное преимущество OpenSSH заключается в том, что он шифрует весь трафик (включая пароли), чтобы эффективно предотвратить перехват соединения и другие атаки, к примеру, такие как ManintheMiddle. Кроме того, OpenSSH предоставляет возможности безопасного туннелирования и несколько методов аутентификации, а также поддерживает все версии протокола SSH.

5. GNU Privacy Guard

GNU Privacy Guard (GnuPG,GPG) - гибридное криптографическое программное обеспечение для шифрования информации и создания электронных цифровых подписей, применяющее различные алгоритмы (RSA, DSA, AES и др.) для решения этой задачи. Программа может использоваться как для симметричного шифрования (для шифровки и

расшифровки задействуется один ключ), так и для ассиметричного шифрования информации (для шифровки и расшифровки задействуется два ключа – публичный и приватный).GPG предоставляет возможность использования различных криптографических алгоритмов с длиной ключа в 1024 или 2048 бит и тем самым позволяет надёжно защитить секретные данные и передавать их.

6. TOR

Tor (The Onion Router) - свободное и открытое программное обеспечение, система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение виртуальных туннелей, предоставляющее передачу данных в зашифрованном виде. Схема работы подразумевает трехкратную защиту данных и анонимизацию трафика. Tor использует так называемую луковую маршрутизацию: данные - это сердцевина лука, а их защита - слои вокруг. Так, каждый из промежуточных серверов Tor снимает свой слой защиты, и только третий, последний из них, достает сердцевину и отправляет запрос в интернет. В дополнение к слоям, Tor шифрует весь сетевой трафик, включая IP-адрес следующего узла. Зашифрованные данные проходят через несколько случайно выбранных ретрансляторов, причем только один слой, содержащий IP-адрес для следующего узла, расшифровывается во время транзита. Конечный узел ретрансляции расшифровывает весь пакет, отправляя данные в его конечный пункт назначения, не раскрывая исходный IP-адрес.

Оружие, наркотики, порнография, услуги киллеров, хакеров, теневой рынок документов, поддельные деньги, отмывание и легализация финансов, ворованные кредитные карточки, вредоносный софт, запрещенная литература – все это является значительной частью ресурсов Tor и создает «благоприятную» среду для преступников и злоумышленников, которая предоставляет им неограниченные возможностидля совершения преступлений.

7. I2P

I2P – это анонимная оверлейная сеть, защищенный протокол обмена данными, основанный на чесночной маршрутизации (более совершенная реализация луковой маршрутизации, используемой в проекте TOR). Решает три основных задачи: невозможность вычислить IP-адрес сервера; избавление от централизованного хранения доменных имен (в роли DNS-серверов выступают множество серверов); тотальное шифрование пакетов данных при передаче их от пользователя к серверу и обратно, что делает бессмысленным перехват пакетов. Используя I2P можно выходить в обычный интернет под чужими IP-адресами, избегая блокировки сайтов в отдельно взятой стране. При этом каждый пакет при передаче шифруется, а затем упаковывается в большой пакет, которая содержит еще несколько таких пакетов для передачи, предназначенных разным узлам. Когда пользователь получает обобщенный пакет, он извлекает из него свой, а остальные пакеты передает дальше. Так как все составные пакеты зашифрованы, то только тот, кому он предназначен, знает, что с ним делать дальше. Промежуточные узлы не знают, что с тем или иным пакетом будет происходить дальше, на следующем узле, и является ли он конечным. Благодаря этому, используя только перехват и анализ пакетов очень трудно определить физическое расположение сервера, а сервер, в свою очередь, ничего не знает о пользователе, который к нему обращается. Перехват осложняется еще и благодаря тому, что каждый пользователь меняет туннель через определенный промежуток времени.

Вышеперечисленные программные обеспечения, основанные на шифровании данных, дают возможность преступникам использовать криптографию в своих корыстных целях. Сочетание этих инструментов намного усложняет процесс их разоблачения правоохранительными органами.

В качестве повышения эффективности противодействия киберпреступности правоохранительные органы должны применять активную деанонимизацию, к примеру: cross-devicetracking (тип атак, позволяющих отслеживать пользователя параллельно через несколько устройств), тайминг-атака по мессенджеру, деанонимизация через сторонние сайты, деанонимизация через путем сопоставления соединений, деанонимизация через

cookies, деанонимизация через Useragent и отпечатки браузера, деанонимизация через файлы-приманки и д.р. Данные способы дают возможность обличить и обнаружить преступника, повышают вероятность их поимки.

Список использованных источников

1. https://cybersecurityventures.com/cybersecurity-almanac-2019/
2. https://genproc.gov.ru/

ТЕХНОЛОГИИ И ИНСТРУМЕНТЫ ПЕРЕХВАТА ТРАФИКА В ЛОКАЛЬНОЙ СЕТИ

Беляева Екатерина Андреевна, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Информация всегда являлась важной составляющей в жизни любого человека. Информация является наиболее значимым ресурсов и фактором в современном мире, который всецело определяет направление развития современных технологий. В связи с этим можно сделать вывод о том, что с развитием технологий и накапливания различной информации развиваются и способы совершения преступлений, которые становятся все анонимнее с каждым днем.

Широкое использование компьютерной техники привело к возникновению задач по хранению, обработке, удалению, обмену цифровыми данными. Появились многочисленные проблемы, относящиеся к аутентичности и анонимности информации.

Различные коммерческие компании многочисленными способами стараются предотвратить несанкционированный доступ к конфиденциальной информации для сохранения своей деятельности.

Применение типичных мер безопасности, например, антивирусов и фаерволов, помогает обеспечить защиту активов организации от внешних угроз, но никак не защиту данных от утечки из-за внутренних угроз, будь то злоумышленник или ошибочные действия сотрудников.

Чтобы обеспечить безопасность данным пришлось прибегнуть к созданию программного обеспечения с помощью которого можно осуществить:

– Полный анализ сетевого траффика для выявления проблем;
– Восстановления потока данных сети;
– Анализ статистика данных сети.

Для успешной работы и выявления всех проблем, анализ трафика должен быть выявлен в 100% виде, чтобы обеспечить все методы анализа для эффективного результата.

Осуществление захвата трафика исполняется при помощи такиой программы как сниффер. Сниффер – это программа или программно-аппаратное устройство, предназначенное для перехвата сетевого трафика в сети.

Компьютерная сеть - это совокупность связанных между собой посредством каналов передачи данных автономных компьютеров с целью обмена информацией и совместного использования ресурсов. При этом под ресурсами понимаются программные и аппаратные средства.

Главным этапом в переходе к компьютерным сетям являлось появление более продвинутых технологий для одновременной работы на нескольких ЭВМ. В связи с этим началось формирование распределённой обработки информации.

Основной целью объединения компьютеров в общую сеть является предоставление пользователям возможности доступа к различным информационным ресурсам (например, документам, программам, базам данных и т.д.), распределенным по этим компьютерам и для совместного использования.

Использование компьютерных сетей дает следующие преимущества:

1) Распределение данных

Распределение данных дает возможность совместного использования различных данных, к примеру баз данных или же любых файлов предоставленных в общий доступ, а также позволяет выполнять разнообразные функции по передаче данных, включая пересылку файлов, обмен данными с внешними запоминающими устройствами.

2) Совместное использование ресурсов

Под ресурсами понимаются программные и аппаратные средства. Объединив в сеть компьютеры организации, можно значительно снизить накладные расходы, связанные с использованием оборудования и периферийных устройств. Общая сеть также позволит существенно уменьшить время, затрачиваемое на управление компьютерным оборудованием.

3) Обеспечение безопасности информации

Компьютерная сеть позволяет обеспечить безопасность тех файлов и ресурсов, к котором есть доступ. В случае проектирования правильной сети появляется возможность отслеживание всех действий касающихся ресурсов сети, что дает полный контроль над всеми, кто работал с данными.

Снифферы - это устройства или программы, которые перехватывают сетевые пакеты данных. Их законная цель - анализировать сетевой трафик и определять потенциально опасные зоны. Например, предположим, что какой-то сегмент вашей сети работает плохо: передача пакетов кажется невероятно медленной или компьютеры внезапно блокируются при загрузке сети. Они используют сниффер, чтобы определить точную причину.

Снифферы существенно отличаются по функциональности и дизайну. Некоторые анализируют только один журнал, а другие могут анализировать сотни. В общем, большинство современных снифферов могут анализировать как минимум один из следующих протоколов:

- Стандартный Ethernet
- TCP / IP
- IPX
- DECNet

При перехвате трафика в рамках оперативных мероприятий важно различать доступ сети и доступ к сетевым службам. Доступ к сети обычно организуется Интернет-провайдером, который использует инфраструктуру оператора связи. Доступ реализуется на всех уровнях модели OSI, от авторизации доступа до сеансового транспорта до общего общедоступного Интернета. Доступ к сетевым службам (такие как электронная почта, чат) могут предоставляться сетевым оператором или сторонней сервисной организацией (поставщиком услуг). Сетевые службы в основном сосредоточены на уровнях 6 и 7, но также могут быть задействованы более низкие уровни (как в коммерческих, так и частных реализациях VPN на основе IPSec). В этой схеме есть еще владелец хоста, крупные сервисы имеют свой хостинг, те кто поменьше арендуют у сторонней организации.

ОТЛИЧИЕ БЕСПЛАТНОЙ АНТИВИРУСНОЙ ПРОГРАММЫ ОТ ПЛАТНОЙ

Бестужев Даниил Дмитриевич, курсант МосУ МВД имени В.Я.Кикотя
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Бесплатное антивирусное программное обеспечение, такое как KasperskyFreeAnti-virus для Windows, предлагает базовую защиту вашего компьютера. Оно помогает защитить ваш компьютер от распространенных вирусов, блокирует опасные файлы и приложения и предупреждает вас о подозрительных веб-сайтах.

Технологии, применяемые в бесплатных антивирусах, могут сильно различаться. KasperskyFreeAnti-virus для Windows использует нашу отмеченную наградами технологию безопасности, которая автоматически в реальном времени получает данные о новых угрозах. Это помогает защитить ваш компьютер от целого ряда онлайн-угроз.

Платные антивирусные решения предлагают более комплексную защиту вашего компьютера.

У каждого антивируса свои преимущества, но качественное платное защитное ПО должно уметь предотвращать вредоносные атаки. Рассматривайте платное антивирусное ПО как проактивный, а не реактивный способ обеспечения безопасности вашего компьютера.

Платное антивирусное ПО также должно контролировать поведение опасных приложений и вредоносных программ, предотвращая заражение до его возникновения.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Бидин Иван Михайлович, курсант МосУ МВД России имени В. Я. Кикотя
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

«Информационная безопасность» — это процесс обеспечения доступности, целостности и конфиденциальности информации.Под «доступностью» понимается соответственно обеспечение доступа к информации.

«Целостность» — это обеспечение достоверности и полноты информации.

«Конфиденциальность» подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.Исходя из целей и выполняемых задач, необходимы будут и различные меры и степени защиты, применимые по каждому из этих трех пунктов. Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее оптимальные средства обеспечения безопасности, для этого рассмотрим основные моменты. Под «Угрозой» понимается потенциальная возможность тем или иным способом нарушить информационную безопасность. Попытка реализации угрозы называется «атакой», а тот, кто реализует данную попытку, называется «злоумышленником». Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем.

Угрозы информационной безопасности, которые наносят наибольший ущерб

1. Угроза непосредственно информационной безопасности:
- Доступность
- Целостность
- Конфиденциальность
2. На какие компоненты угрозы нацелены:
- Данные
- Программы
- Аппаратура
- Поддерживающая инфраструктура
3. По способу осуществления:
- Случайные или преднамеренные
- Природного или техногенного характера
4. По расположению источника угрозы бывают:
- Внутренние
- Внешние

Понятие «угроза» в разных ситуациях зачастую трактуется по-разному. И необходимые меры безопасности будут разными.

Применимо к виртуальным серверам, угрозы, которые необходимо принимать во внимание это — угроза доступности, конфиденциальности и целостность данных. За возможность осуществления угроз направленных на конфиденциальность и целостность данных, не связанные с аппаратной или инфраструктурной составляющей, несется прямая и самостоятельная ответственность. В том числе как и применение необходимых мер. защиты. На угрозы направленные на уязвимости используемых программ, зачастую пользователь не сможете повлиять, кроме как не использовать данные программы. Допускается использование данных программ только в случае если реализация угроз используя

уязвимости этих программ, либо не целесообразна с точки зрения злоумышленника, либо не имеет для пользователя существенных потерь.

Угрозы непосредственно информационной безопасности

К основным угрозам доступности можно отнести

1.Внутренний отказ информационной системы;

2.Отказ поддерживающей инфраструктуры.

Основными источниками внутренних отказов являются:

- Нарушение (случайное или умышленное) от установленных правил эксплуатации
- Выход системы из штатного режима эксплуатации в силу случайных или преднамеренных действий пользователей (превышение расчетного числа запросов, чрезмерный объем обрабатываемой информации и т.п.)
- Ошибки при (пере)конфигурировании системы
- Вредоносное программное обеспечение
- Отказы программного и аппаратного обеспечения
- Разрушение данных
- Разрушение или повреждение аппаратуры

По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы:

- Нарушение работы (случайное или умышленное) систем связи, электропитания, водо- и/или теплоснабжения, кондиционирования;
- Разрушение или повреждение помещений;
- Невозможность или нежелание обслуживающего персонала и/или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.).

Основные угрозы целостности

Можно разделить на угрозы статической целостности и угрозы динамической целостности.

Так же стоит разделять на угрозы целостности служебной информации и содержательных данных. Под служебной информацией понимаются пароли для доступа, маршруты передачи данных в локальной сети и подобная информация. Чаще всего и практически во всех случаях злоумышленником осознанно или нет, оказывается сотрудник организации, который знаком с режимом работы и мерами защиты.

С целью нарушения статической целостности злоумышленник может:

- Ввести неверные данные
- Изменить данные

Угрозами динамической целостности являются, переупорядочение, кража, дублирование данных или внесение дополнительных сообщений.

Конфиденциальную информацию можно разделить на предметную и служебную. Служебная информация (например, пароли пользователей) не относится к определенной предметной области, в информационной системе она играет техническую роль, но ее раскрытие особенно опасно, поскольку оно чревато получением несанкционированного доступа ко всей информации, в том числе предметной.

Даже если информация хранится в компьютере или предназначена для компьютерного использования, угрозы ее конфиденциальности могут носить некомпьютерный и вообще нетехнический характер.

К неприятным угрозам, от которых трудно защищаться, можно отнести злоупотребление полномочиями. На многих типах систем привилегированный пользователь (например системный администратор) способен прочитать любой (незашифрованный) файл, получить доступ к почте любого пользователя и т.д. Другой пример — нанесение ущерба при сервисном обслуживании. Обычно сервисный инженер получает неограниченный доступ к

оборудованию и имеет возможность действовать в обход программных защитных механизмов.

Для применения наиболее оптимальных мер по защите, необходимо провести оценку не только угроз информационной безопасности но и возможного ущерба, для этого используют характеристику приемлемости, таким образом, возможный ущерб определяется как приемлемый или неприемлемым. Для этого полезно утвердить собственные критерии допустимости ущерба в денежной или иной форме.
Каждый кто приступает к организации информационной безопасности, должен ответить на три основных вопроса:

1.Что защищать?

2.От кого защищать, какие виды угроз являются превалирующими: внешние или внутренние?

3.Как защищать, какими методами и средствами?

Принимая все выше сказанное во внимание, можно наиболее полно оценить актуальность, возможность и критичность угроз. Оценив всю необходимую информацию и взвесив все «за» и «против» можно подобрать наиболее эффективные и оптимальные методы и средства защиты.

ЗАЩИТА КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ, КАК СПОСОБ ПОДДЕРЖАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Богданова Анастасия Максимовна, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В современном мире существуют множество областей и отраслей жизнедеятельности общества, которые требуют особенного подхода в использовании. Ежедневно человечество сталкивается с такими проблемами, как: грабежи, случайные связи с незнакомыми людьми, потеря вещей. Информатизация нашего общества продолжается в достаточно быстром темпе. Пользователей информационными системами становится все больше. Количество информационного ресурса увеличивается в геометрической прогрессии. Немаловажным является и прослушивание телефонных разговоров, чтение личной информации в социальных сетях и просто слежение за действиями определенных лиц.

С одной стороны, информация стоит денег. Утечка или потеря информации ведет к материальному ущербу. С другой стороны, информация - это управление. Несанкционированное вмешательство в управление может иметь катастрофические последствия для объекта управления - производства, транспортировки, военного дела. Необходимость изучения уровня защиты конфиденциальности информации в информационной системе на всех этапах ее жизненного цикла определяется необходимостью принятия рационального управленческого решения для обеспечения защиты информации, в том числе ее конфиденциальности. Актуальность проблемы усугубляется тем фактом, что обеспечение адекватной защиты конфиденциальности информации важно для успешного функционирования самой информационной системы и требует выделения значительного ресурса. Поэтому требование по обеспечению эффективности функционирования подсистемы защиты конфиденциальности в составе системы защиты информации является одним из ключевых.

Информационные угрозы, как правило, направлены на получение информации по определенным объектам, чаще всего это конфиденциальная информация различных организаций и отдельных людей. При разглашении коммерческой тайны предприятие или фирма может сильно ухудшить свою экономическую ситуацию.

Каналами утечки, как было упомянуто выше, могут быть локальные пользователи, но присутствует риск потери данных со стороны злоумышленников особой секретности. Таковыми являются хакеры, способные дистанционно похитить информацию, которая находится под неразглашением.

Большинство внешних угроз возникает из-за неправильной конфигурации систем информационной безопасности или человеческих факторов. Примером является атака Stegosploit. Атака была начата в 2015 году индийским исследователем безопасности Саумилом Шахом. Атака включает в себя сокрытие исполняемого вредоносного кода в пикселе изображения, и если пользователь решит загрузить изображение в браузер, он нарушит систему.

В настоящее время в типовом отделе компании положение о коммерческой тайне и конфиденциальной информации, а также система, обеспечивающая защиту конфиденциальной информации, могут оказать негативное влияние на информационную безопасность. Поскольку компания предоставляет свои услуги в течение многих лет, вы можете оценить большой объем данных, которые необходимо защитить.

В правовом аспекте информационная безопасность может быть нарушена при умышленном или случайном нарушении свойств информационной среды. Менеджмент

хозяйствующего субъекта столкнется тогда с уничтожением или модификацией информации.

Стоит отметить, что подобного рода развитие обстоятельств может привести к непредсказуемым исходам. Так, к примеру, каждый злоумышленник способен тайным путем остаться не замеченным в содеянном правонарушении, однако место его работы, естественно теряет прежнюю организационную силу, что на руку конкурентам. Чтобы избежать подобных проблем, каждый владелец компании или организации должен строго соблюдать следующие правила:

- четкая формулировка кадровой политики, проведение работ по обеспечению лояльности персонала;
- обсуждение и определение политики ИБ в отношении конфиденциальной информации;
- организационные меры по обеспечению юридической ответственности за разглашение конфиденциальной информации;
- ограничение доступа к конфиденциальной информации в соответствии с политикой. Устранение путей утечки больших объемов информации;
- контроль, архивирование информационных потоков. Расследование случаев утечки информации по обвинению авторов, даже преступников; [8]

С частью локального хищения дела обстоят куда проще, чем в области утери информации дистанционно. Не трудно догадаться, речь пойдет об утечки конфиденциальной информации путем взлома систем. Взлом систем производит специалист компьютерной области с высоким уровнем квалификации, способный взламывать защиту компьютерной системы. Каждый, кто использует компьютер или ноутбук, имеет на своем компьютере что-то, что никто не должен видеть или это не должно никого беспокоить. Взлом компьютерных систем и вторжение третьих лиц, таких как хакеры, обычно становятся настоящей проблемой. ПК могут в настоящее время содержать контент, который не должен быть доступен другим. Сначала он собирает информацию о предполагаемой цели, находит лучший план атаки, а затем атакует возможные уязвимости (уязвимости) в системе. Поэтому в это время не лишне безопасно играть, то есть всегда устанавливать последнюю версию антивируса и постоянно обновлять ее. Вам необходимо постоянно следить за обновлениями браузера. Потому что разработчики браузеров постоянно совершенствуют свои браузеры, что повышает защиту компьютера и снижает риск взлома компьютера.

На сегодняшний день в ПК могут находиться материалы, которые не должны быть доступны другим людям. Вначале он собирает информацию о намеченной цели, выясняет лучший план атаки, а затем атакует возможные уязвимости (слабые места) в системе.

Поэтому, в нынешнее время, не лишним будет перестраховаться, то есть всегда ставить новейшую версию антивирусной программы и постоянно её обновлять, необходимо постоянно наблюдать за обновлением браузера. Для тех, кто пользуется роутерами, в целях безопасности, нужно установить пароль. Кроме того, для защиты компьютера от хакеров, нужно проверять на подлинность URL. Чаще всего, именно ошибкой, всего в одну букву пользуются взломщики, для получения пароля. [6]

Как и в любой другой системе, призванной защищать и предотвращать, одним из первых средств является аудит, включающий в себя сбор и анализ событий, а также механизмы обратной связи (оповещение о критических событиях, автоматический запуск необходимых процессов защиты).

Средства обеспечения безопасности должны быть адекватны степени конфиденциальности данных и требованиям к их защите. Есть места, где необходима защита любой ценой, но в большинстве случаев стоимость внедрения и сопровождения систем ИБ не должна превышать возможные убытки от потенциальных проблем.

Одним из основных средств защиты информации является шифрование, которое позволяет шифровать информацию и, таким образом, защищать ее от чтения и незаметных изменений при хранении и передаче по каналам связи. По мере появления новых

информационных технологий перед их средствами защиты появляются многообещающие области для разработки и внедрения систем защиты информации.

В настоящее время широкое распространение получили облачные хранилища, такие как Яндекс.Диск, Dropbox и Google Drive.

Выбирая удобное место для хранения, пользователь обращает внимание на количество свободного места, доступного бесплатно, теряя из виду безопасность. Например, диск «Яндекс», который является одним из самых популярных средств архивирования и услуг, которым пользуются более 175 миллионов человек, не шифрует файлы при загрузке в облачное хранилище. Следовательно, данные в этой папке могут использовать все, кто имеет доступ к устройству или знает имя пользователя / пароль.

Существует два способа доступа к данным: через браузер и установку клиентской программы на компьютер. В первом случае доступ может быть ограничен выходом из учетной записи, во втором случае файлы синхронизируются и физически доступны на устройстве. Второй вариант предпочтительнее с точки зрения удобства для пользователя, поскольку работа с ними ничем не отличается от работы с картой памяти.

Проект намеревается создать в облачном хранилище папку, к которой имеет доступ только владелец. Данные доступны только когда владелец находится на компьютере. Наш метод исключает использование украденного пароля пользователя из-за модифицированной системы аутентификации.

Изменение в системе аутентификации заключается в том, что вам необходимо подключить мобильный телефон (идентификационный ключ) к компьютеру и ввести пароль для подтверждения личности владельца. Когда телефон отключен, папка автоматически закрывается и шифруется.

Дополнительно: в случае потери мобильного телефона пользователь уведомляет службу, которая, в свою очередь, блокирует доступ к папке с помощью потерянного телефона и предлагает пользователю сгенерировать новые идентификаторы с использованием мастер-ключа (например, флешка).

Для вычислений (в MD5/MD6) инициализируются 4 переменных размером по 32 бита и задаются начальные значения шестнадцатеричными числами (порядок байтов тот же - littleendian, сначала младший байт): ABCD, а модификация предполагает включение 5-й переменной E, что приведет к увеличению раундов, а значит, к более сложному криптоанализу.

Данные доступны только если владелец находится на компьютере. Наша методология исключает использование украденного пароля пользователя из-за модифицированной системы аутентификации.

Одна из модификаций системы аутентификации заключается в том, что для подтверждения личности владельца необходимо подключить мобильный телефон (который является ключом идентификации) к компьютеру и ввести пароль. Когда телефон отключен, папка автоматически закрывается и шифруется.

Кроме того, в случае потери мобильного телефона пользователь уведомляет службу, которая, в свою очередь, блокирует доступ к папке, используя потерянный телефон, и просит пользователя сгенерировать новые идентификаторы, используя первичный ключ (например, флешка).

Следующим наиболее важным аспектом в организации информационной безопасности в процессинговых центрах является защита на уровне операционных систем, приложений и баз данных. Основная задача должна быть выполнена: «Критические данные должны быть доступны только авторизованным лицам и только в порядке, разрешенном правилами безопасности». Это, в частности, подразумевает использование механизмов, которые контролируют запуск только авторизованных программ авторизованными пользователями (решения типа CA AccessControl, системы типа hostbasedintrusionprevention).

В заключении хотелось бы отметить, что защита конфиденциальной информации является самым важным аспектом в области хранения данных. Если информация будет

содержать сведения о конкурентах, то следует ограничить круг проинформированных о ней сотрудников во избежание непредвиденных обстоятельств. Объединение и соблюдение в совокупности всех перечисленных правил поможет к достижению обеспечения максимального уровня защиты конфиденциальной информации.

Список используемой литературы:

1. Бабаш А.В. Информационная безопасность. Учебное пособие / А.В. Бабаш, Е.К.Баранова, Ю.Н. Мельников. - М.: КноРус, 2018. - 136с.
2. Егорова Ю.Н. Информационная безопасность: учебное пособие. / Ю.Н. Егорова– Чебоксары: Изд-во Чувашского ун-та, 2015. – 131 с.
3. Карзаева Н.Н. Основы экономической безопасности. / Н.Н. Карзаева – М.: ИНФРА-М, 2017. – 275с.
4. Исследование утечек информации за первое полугодие 2015 года [Электронный ресурс] URL: http://www.infowatch.ru/analytics/reports/16340.
5. Самые громкие утечки информации 2019 года [Электронный ресурс] URL: https://searchinform.ru/news/world-news/.
6. Бабенко Л.К., Ищукова Е.А. Современные алгоритмы блочного шифрования и методы их анализа. - М.: Гелиос АРВ,12006. -376 с.

ПОСТРОЕНИЕ ВНУТРЕННЕЙ СОИБ (СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ) НА ПРЕДПРИЯТИИ

Большунов Егор Геннадьевич, курсант МосУ МВД России имени В.Я. Кикотя
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Построение комплексной системы информационной безопасности (КСИБ) в крупной компании представляет собой сложный процесс, связанный с изменением существующих бизнес-процессов, функционала подразделений, а также перераспределением ответственности между руководителями разного уровня подчиненности. Любой новый процесс, а тем более новое подразделение, очень тяжело вклинить в нормально работающую и приносящую прибыль компанию, а процесс контроля, информационного контроля, и вообще запредельная задача. На практике приходится сталкиваться не столько с техническими трудностями реализации, сколько с коммуникациями на уровне операционного управления. Никто и никогда из директоров CIO не захочет добровольно устанавливать у себя на локальной вычислительной сети системы контроля трафика, а тем более исполнять какие-то правила информационной безопасности написанные и спущенные с верху, поэтому построить КСИБ используя добровольно-принудительные меры, не поругавшись с CIO и остаться на работе – это искусство.

Цель проводимого в работе исследования – описать, как построить КСИБ в крупной компании, с какими трудностями предстоит столкнуться и как их преодолеть при реализации проекта.

Основные задачи, решаемые в процессе работы:

- внедрить документацию по информационной безопасности;
- организовать процесс управления и контроля доступа к информационным ресурсам;
- сформировать подразделение информационной безопасности;
- организовать контроль над информацией.

Текущее положение в крупных компаниях характеризует несколько ключевых моментов. Один из моментов, это сокращение расходов. Безопасность – это расходы всегда. Снизить затраты на безопасность используя внутренние резервы компании можно и нужно. С одной стороны, это оказывает влияние на уменьшение себестоимости внедряемых организационно-технических решений. С другой стороны, сокращение затрат на безопасность принимаются у руководителей компании как – это что-то новое и соответственно вызывает интерес. Если интересно руководителю, значит, проект имеет шансы жить и развиваться. Руководство компании должно знать, как происходит доступ к той или иной финансово значимой информации в компании, как эта информация храниться, и кто конкретно отвечает за нормальное функционирование тех или иных информационных систем. Доступна, актуальна и информативна ли информация, курсирующая по локально вычислительной сети компании. При отсутствии КСИБ могут быть пропущены действительно хорошие возможности сокращения затрат за счет простого управления информационных потоков. Необходимость тщательного анализа текущей ситуации с информационной безопасностью становится жизненно необходимым, бизнес- критичным процессом, в крупной компании. КСИБ - система предоставляет сотрудникам целевой, персонализированный доступ к информации, которая способна сделать их работу более эффективной, и охватывает все основные направления внутри компании: финансы, маркетинг, товародвижение, логистику, управление персоналом, информационные

технологии. Существуют методики и разработаны стандарты в области информационной безопасности, где все просто и понятно написано, как это сделать, в теории. Казалось бы, что проще взять стандарт и применить его в компании, ведь вроде все требования идентичны, но на практике это часто не так. Понятие информационная безопасность может по-разному пониматься в разных департаментах одной компании. Поэтому важным видится единое понимание сотрудников компании, что такое информационная безопасность. Зачастую простое информирование о работе подразделения информационной безопасности, распространенной на всю организацию, позволяет устранить разную трактовку этого понятия. Помимо этого, нужны гибкие инструменты интеграции в компании нового подразделения и многое зависит и от харизматичности руководителя информационной безопасности. Именно ему создавать положительный образ нового подразделения. Крайне важным для руководителя ИБ организовать «центр контроля» за информационными потоками, необходимо добиться, чтобы во всех решениях, связанных с доступом к информационным ресурсам, созданием новых информационных ресурсов, передачей информации третьим лицам, уничтожением информационных ресурсов, участвовало подразделение информационной безопасности.

Подразделение информационной безопасности должно быть подотчетна руководителям высшего звена - директору по безопасности или исполнительному директору, с тем, чтобы обеспечить прямую и короткую связь с руководителем компании. События на информационной сети происходят часто и не все являются следствием существующих в компании бизнес-процессов, часто информация уходит за пределы компании скрытно, руководитель об этом должен знать первым. Подчинение информационной безопасности подразделению ИТ недопустимо!!! Контролер и подконтрольный не должен быть в одном подразделении.

Построение КСИБ в компании предоставляет множество преимуществ для представителей ИБ, IT-структур и бизнеса. Офицеры безопасности получают возможность контролировать права доступа в информационных системах: в любой момент времени знать, кто, куда, когда и какой доступ имел. Техническая составляющая КСИБ позволяет оперативно отслеживать и расследовать инциденты информационной безопасности, связанные с наличием избыточных привилегий, выполнять регламенты разделения ответственности и инвентаризации прав доступа пользователей. КСИБ позволяет значительно ускорить процессы управления доступом, тем самым это способ повысить эффективность работы сотрудников, а также повысить прозрачность процессов управления доступом.

ПРОМЫШЛЕННЫЕ РОБОТЫ В ГОРНОДОБЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ

Бугаков Александр Андреевич, студент 3-го курс
Научный руководитель Комарова Юлия Викторовна, преподаватель 1 категории
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Горнодобывающая промышленность является одной из самых важных отраслей народного хозяйства Российской Федерации. Добыча железной руды в России составляет 8% от мировой добычи.

Одной из самых больших проблем горнодобывающих предприятий – это ухудшение природных и горно-геологических условий в месте разработки природных ископаемых. Рентабельность предприятия падает из-за увеличения затрат на обеспечение безопасных условий разработки и на экологические мероприятия.

Актуальность темы заключается в исследовании обеспечения необходимой безопасности горнодобывающих работ инеобходимости внедрить роботов. В данной работе представлен обзор и анализ роботизированных предложений для горнодобывающей промышленности.

Целью исследования является выявить необходимость внедрения роботов в горнодобывающую промышленность.

Внедрение роботизированных технологий увеличивает эффективность работы персонала, существенно снижает затраты на безопасность, повышает производительность и управляемость процессов.

В зарубежных странах роботизация добывающих компаний идет по разнообразным направлениям. С конца 2016 года началось массовое внедрение беспилотных систем в добывающем секторе.Оченьактивно начинается использование автономно работающих грузовиков, буровых установок и даже транспортных поездов. Применение беспилотных систем повышают эффективность добычи полезных ископаемых, сокращают потребность в персонале, что особенно важно для развитых стран с высоким уровнем средней заработной платы [1].

Лидирующий канадский нефтедобытчик "SuncorEnergy" испытывает самосвалы-роботы при добыче кварцевого песка.В Австралии, шахты концерна RioTinto используют 73 роботизированных грузовика, которые получают сырье с роботизированных буровых установок, и подвозят их к поездам. В Германии компания "KUKA Roboter" применяют роботизированный манипулятор для установки арочных крепей. Немецкая фирма TopTec разработала демонтажного робота для выполнения сложных горнопромышленных работ. Их технику можно использовать в любых замкнутых помещениях с ровной или не ровной поверхностью. В Испании применяется роботизированный проходческий комбайн Alpine AM-105ex (рисунок 1) разработанный фирмой "SANDVIK".

Рисунок 1 - Проходческий комбайн Alpine AM-105ex.

Французская фирма "Montabert" разработала роботизированную бурильную установку "Robofore", обеспечивающую бурение по заданной программе с автоматическими операциями бурения и перестановки двух манипуляторов. Шведская фирма "NitroNobelMec".создала мобильные манипуляторы HF-51 и EG-33 с дистанционным управлением для заряжания взрывчатым веществом скважин в незакрепленных выработках. Шведская компания BrokkAB разработала и представила демонтажные серийные роботы которые способны производить бурение скважин в шахтах без тяжелой техники, разработку горных пород в ограниченных пространствах, оборку за-колов, дробление негабарита. Данные роботы (рисунок 2)оснащены маневренным манипулятором, который имеет диапазон оборота от 270г до 360г [2]. Это позволяет производить работы в различных плоскостях, например горизонтальное бурение.

Рисунок 2 - Демонтажные серийные роботы.

Свой вклад по внедрению роботизации в горнодобывающую промышленность вносят и страны СНГ. Так, например, украинский новокраматорский машиностроительный завод создал угольный проходческий комбайн П-110 (рисунок 3), который оснащен системами самодиагностики и системой радиоуправления на базе микропроцессоров. [3].

Рисунок 3 - Проходческий комбайн П-110.

Белорусский автозавод совместно с российской "ВИСТ-Групп" разработал и активно внедряет интеллектуальные карьерные самосвалы, которыми управляет дистанционно оператор.Современное оборудование, которым оснащены новые карьерные самосвалы, позволяет эксплуатировать машины в условиях повышенных нагрузок и обеспечить высокую надежность и безопасность техники.

Ученые из Перми разработали "робот-шахтера", который по их идее должен выполнять все необходимые операции в шахте [4]. Его можно применять как в буровзрывных работах, так и при установочно-наладочных работах. Одним из преимуществ данного робота является то, что он малогабаритен с рукой-манипулятором и располагается на движущей платформе.

Резидент «Сколково» компания "Вист Майнинг Технолоджи" разработала и предлагает технологии для создания роботизированных участков горных работ [5]. На таких участках добычу будет вести роботизированная и дистанционноуправляемая техника - самосвалы, экскаваторы, погрузчики, бульдозеры, буровые станки, автономный железнодорожный транспорт.

В автопарке АО «Стойленского ГОКа» появились автосамосвалы с частично роботизированными технолгиями. Жидкокристаллический монитор, установленный в кабине автосамосвала, позволяет водителю контролировать остаток топлива, текущую грузоподъемность и показатель давления шин.Напалубе самосвала установлено трёхсекционное цифровое табло, на котором отражается загрузка автосамосвала в тоннах, что позволяет детальнее контролировать погрузку горной массы. В кабине установлены система климат-контроля и система кругового обзора при движении задним ходом.Все новые автосамосвалы включены в автоматическую систему диспетчеризации «Карьер».Системы контроля усталости водителя и система видеонаблюдения, которая позволяет следить в режиме онлайн и оффлайн за ситуацией на дороге и за действиями водителя. Компьютер отслеживает положение автосамосвала, объем перевозки, содержание железа в руде на различных участках карьера и на основе этих данных система диспетчеризации вычисляет оптимальный трафик.

Таким образом, внедрение роботизированных технологий позволит:

- расширить добычу в шахтах, поскольку роботы могут работать в любых условиях;
- увеличить производительность, так какдобычу можно будет вести в непрерывном, круглосуточном режиме;
- увеличить условия безопасности вшахтах, поскольку роботизированные шахты не потребуют регулярного присутствия людей под землей;
- расширить ассортимент добываемых природных ископаемых, можно добывать кроме угля еще и метан;
- обеспечить надежную и безопасную работу по перевозки горных масс;
- улучшить условия работы рабочих горнодобывающих предприятий.

Список использованных источников

1. Умное производство [Электронный ресурс]: многопредмет. науч. журн. / Мод.реал. сект. произв. – Электрон. журн. –Тверь, 2017. – режим доступа к журн.: http://www.umpro.ru/.

2. RoboTrends [Электронный ресурс]: науч. инт. журн. / Разр. роб.предл. – Электрон. журн. –Москва, 2017.–режим доступа к журн.: http://robotrends.ru/

3. А.Д. Мехтиев. Роботизированный комплекс / А.Д. Мехтиев//Когнитивная робототехника межд.научн.конф. – 2016. - № 12. – С. 34-35.

4. Поезжаева Е.В. Роботизация горного дела / Е.В. Поезжаева // Науковедение. – 2016. - № 7. – С. 52-57.

5. Владимиров Д.Я. Интеллектуальный карьер: эволюция или революция [Текст] / Д.Я. Владимиров //Открытые горные работы в XXI веке. . – 2016. - № 12. – С. 50-55.

ВЛИЯНИЕ СПОРТА НА КУЛЬТУРУ ОБЩЕСТВА

Буцкая Полина Владимировна, Щурова Елизавета Валерьевна, студенты 1-го курса
Научный руководитель Бояришев Вадим Викторович, преподаватель высшей категории

Общественная культура сейчас особенно интересует российских исследователей. В настоящее время внимания заслуживают трудности восстановления ценностей общества, в ряду каких присутствует и спорт со своей многозначной сущностью.

Отношение спорта и культуры предугадывает воздействие здорового образа жизни не только на физиологическое состояние, самочувствие человека, но и на духовный мир личности. Таким образом, актуальность исследования обусловлена интересом к влиянию спортивных организаций на культуру общественных отношений.

В связи с актуальностью темы целью нашего исследования является установление особенностей влияния физической культуры и спорта на российское общество.

Физическая культура и спорт, являясь составляющими культуры, области социальной деятельности, представляют собой совокупность духовных и материальных ценностей, используемых обществом в целях физического развития человека, укрепления его здоровья и совершенствования его двигательной активности, спортивной практики подготовки человека к соревнованиям.

Физическая культура, являясь одной из граней общей культуры человека, его здорового образа жизни, во многом определяет поведение человека в учебе, на производстве, способствует решению социально-экономических, воспитательных и оздоровительных задач.

Важными социальными задачами, для решения которых необходимо вовлечение людей в сферу физической культуры, считаются вредные привязанности населения государства (алкоголизм, наркомания, табакокурение). На данный момент табакокурение считается одной из самых популярных привычек в России – ей подвержены более 80% населения государства. В число курильщиков также входят женщины, которые, зачастую, не изменяют этой привычке и во время беременности или кормления детей, и подростки.

Физическая культура — это уникальное социальное явление, которое способно при правильном подходе объединять общество, укреплять на основе общедоступных норм его нравственное и физическое здоровье. Эффективное использование возможностей спорта помогает сохранению и укреплению здоровья людей, в профилактической работе, в борьбе с наркоманией, пьянством, курением, особенно среди молодежи.[1] Спорт это одно из главных средств воспитания движений, развития необходимых человеку двигательных физических качеств. «Если заниматься физическими упражнениями — нет никакой нужды в употреблении лекарств, принимаемых при разных болезнях, если в то же время соблюдать все прочие предписания нормального режима» (Авиценна).[3]

В связи с этим, в настоящее время наиболее важным направлением является поиск эффективных технологий разработки средств физической культуры и спорта, обладающих универсальной способностью в комплексе решать проблемы повышения уровня здоровья населения, формировать здоровый морально-психологический климат в обществе.

Обозначим следующие возможные пути вовлечения людей в сферу физической культуры:

1) Реклама здорового образа жизни. Она обязана подчеркивать то, что физическая активность считается наилучшим средством снятия стресса, способствует отвлечению и отдыху организма. Для детей реклама содержит другой смысл, значительно эффективнее мнение авторитетных людей, тех, кому дети стараются подражать. Проводить мероприятия с участием спортсменов, артистов, и иных общественных деятелей, которые станут пропагандировать здоровый образ жизни, занятия спортом и отказ от вредных привычек.

2) Спортивные организации должны гарантировать каждому заинтересованному необходимую численность спортивных учреждений для привлечения людей в сферу физической культуры.

3) Проводить агитацию молодёжи, начиная с младших классов начальной школы. Пропагандировать здоровый образ жизни для детей, проводить спортивные события в учебных заведениях в масштабах района и города.

4) Для старшего поколения пропаганда вероятна на уровне всевозможных общественных и целительных учреждений.

5) Необходимо проводить соревнования и спортивные праздники, целью которых является пропаганда здорового образа жизни.

6) Мотивировать людей к отказу от вредных привычек посредством введения штрафов за курение на рабочих местах.

Таким образом, спорт способен выступать двигателем борьбы с социальными и общественными проблемами. Они способны содействовать уменьшению числа приверженцев вредных привычек, сокращению заболеваний и поддержанию формы у каждого человека. Физическая культура также способствует решению социальных проблем.[1] Также она содействует воспитанию здоровых и сильных людей, с закреплёнными правильными моральными устоями, способных развиваться и трудиться на благо общества и государства. [2]

Список использованных источников

1. Паначев В. Спорт и личность / В. Паначев // СОЦИС. - 2007. - № 11. - С.125-129

2. Чернов И.В., Ревунов Р.В. Организация учебно-тренировочного процесса по физической культуре в высшем учебном заведении (на примере тяжёлой атлетики). М.: Лань, 2019.

3. Качанов Л. Н., Шапекова Н., Марчибаева У. Лечебная физическая культура и массаж. Учебник. М.: Фолиант, 2018.

СОВРЕМЕННАЯ НАУКА

Бучукова Лидия Дмитриевна, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Научно-исследовательская работа — работа научного характера, связанная с научным поиском, проведением исследований, экспериментами в целях расширения имеющихся и получения новых знаний, проверки научных гипотез, установления закономерностей, проявляющихся в природе и в обществе, научных обобщений, научного обоснования проектов.

Принципиальным отличием содержания современного образования является его нацеленность на развитие творческой, социально-активной личности, выявление её познавательных интересов и потребностей выдвигают задачу развития познавательных способностей, активизации познавательной самостоятельности обучаемых.

Активизация познавательной самостоятельности складывается из целенаправленного взаимодействия педагогов и обучающихся, осуществляемого в учебной и внеучебной работе. Внеучебную деятельность необходимо организовать так, чтобы она служила продолжением учебной работы и являлась полноправным компонентом образовательного процесса, направленного на систематическое образование обучающихся и активизации их познавательной самостоятельности.

К формам и методам внеучебной работы, благодаря которому осуществляется процесс целенаправленной активизации познавательной самостоятельности, относят научно-исследовательскую и проектную деятельность студентов, экспедиции, полевые практики, научно-практические конференции, олимпиады, тематические вечера и другие.

Мотивация научно-исследовательской работы предшествует приобщению студентов к этому виду деятельности. Именно на этой стадии каждый участник научно-исследовательской работы должен увидеть её будущее и вполне конкретные результаты.

Исследовательская работа — это первый шаг студентов в науку. Как показывает опыт, она способствует возникновению и закреплению интереса к творческой деятельности, является важным средством активизации познавательной самостоятельности учащихся.

Метод проектов не только позволяет развивать интерес обучаемых к преподаваемой дисциплинам и обеспечивает высокий уровень их теоретической подготовки, но и интенсифицирует процесс активизации познавательной самостоятельности студентов. Как показывает опыт, внеучебная деятельность студентов, представленная разнообразными формами и методами, играет в процессе активизации познавательной самостоятельности не менее важную роль, чем учебная работа.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Вахрушева Дарья Сергеевна, курсант 1-го курса.
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Заражение ПК не происходит при загрузке зараженного Web-сайта. То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов "попутной загрузки" возможно уже на протяжении многих лет. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке".Во-первых, Web-сайты, созданные специально с целью заражения ПК.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое заражение ПК вредоносной программой. Преимуществом данного способа для киберпреступников является то, что им не приходится рекламировать Web-сайт. Для дальнейшей манипуляции данным Web-сайтом злоумышленникам необходимо в него внедриться. Если Web-сайт хорошо защищен, то осуществить такое внедрение очень сложно.

Что происходит с информационной безопасностью в мире?

* Информационные технологии стали частью повседневной жизни и имеют глобальный характер. А если эффективно их использовать — можно ускорить экономическое развитие государства.
* Чем опасен глобальный характер информации. Тем, что ее все чаще используются для достижения незаконных геополитических, военно-политических, а также террористических, экстремистских, криминальных целей в ущерб международной безопасности.
* Воздействуя на информацию, можно вести войну нового поколения. Ряд зарубежных стран наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях.
* Спецслужбы воруют гостайну, военные и научные секреты. Активизировались организации, специализирующиеся на технической разведке в отношении российских госорганов, научных организаций, предприятий оборонки.
* Информационные атаки угрожают национальной безопасности. Спецслужбы отдельных государств оказывают «информационно-психологическое воздействие», чем пытаются дестабилизировать ситуацию в странах различных регионов мира, подорвать суверенитет и нарушить территориальную целостность уязвимых стран.
* Интернетом нельзя управлять справедливо. Ресурсы, необходимые для безопасного и устойчивого функционирования интернета, распределены в мире неравномерно. Это означает, что управлять глобальным интернетом на принципах доверия и справедливости невозможно в принципе.

Как Россия будет защищаться от угроз в сфере информационной безопасности в области обороны:

* будет сдерживать и предотвращать военные конфликты, которые может спровоцировать применение информационных технологий;

* будет совершенствовать систему информационной безопасности армии, причем не только защитного характера, но и атакующие силы («силы и средства информационного противоборства»);
* будет защищать интересы союзников России в информационной сфере;
* будет нейтрализовывать информационно-психологическое воздействие, направленного «на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества».

ИССЛЕДОВАНИЕ 5G ТЕХНОЛОГИЙ

Гаус Глеб Романович, командир отделения 4 курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В наступающем году телекоммуникационные компании должны играть еще большую роль, поскольку беспроводная технология 5G начинает набирать обороты как среди предприятий, так и среди потребителей. В частности, 5G обещает предоставить предприятиям беспрецедентную скорость в реальном времени, понимание и контроль над их активами, продуктами и услугами. Это также может предоставить новые возможности для радикального изменения того, как они работают и предоставляют новые продукты и услуги.

Во многих отношениях это представляет собой серьезный сдвиг для телекоммуникационных компаний. В то время как телекоммуникационная модель перехода потребителей на беспроводные технологии следующего поколения уже доказана, провайдеры должны разработать бизнес-модель для решения корпоративных рынков, которые выиграют от передовых беспроводных технологий, таких как 5G. Это, скорее всего, потребует изучения и разработки новых операционных и бизнес-моделей, требующих более тесного сотрудничества со сторонними партнерами для создания комплексных корпоративных приложений, удовлетворяющих разрозненные потребности конкретных отраслей.

Поскольку 5G, скорее всего, вызовет инновационные бизнес-модели, которые получат широкое распространение, телекоммуникационные провайдеры должны стремиться помочь корпоративным клиентам получить первые преимущества в определении и разработке инновационных бизнес-моделей, которые могут нарушить их отрасли.

Хорошая новость для телекоммуникационных провайдеров и технологических компаний заключается в том, что большинство компаний уже понимают важность использования передовых технологий беспроводной сети для стимулирования будущего роста. В недавнем исследовании Deloitteadvancedwirelessadoption" предприятия, строящие свое будущее с помощью 5G и Wi-Fi 6», те, кто использует и тестирует 5G и/или Wi-Fi 6, видят огромный потенциал—86% опрошенных сетевых руководителей считают, что advancedwireless преобразит их организацию в течение трех лет.

Более девяти из десяти таких руководителей считают передовые беспроводные технологии «очень» или «критически» важными для их успеха в бизнесе.

Рыночные возможности огромны: по оценкам Ассоциации глобальной системы мобильной связи, 5G принесет $700 млрд экономической стоимости, при этом предприятия, представляющие 68% рынка, во главе с розничными, государственными и финансовыми приложениями.

Ключевые возможности для роста

Возможности 5G способны произвести революцию в любой отрасли-от производства до здравоохранения и государственного управления. Чтобы полностью реализовать перспективные передовые беспроводные технологии, такие как 5G, телекоммуникационные провайдеры должны делать больше, чем просто предоставлять коммуникационную сеть—важно, чтобы они также объединили все необходимые возможности. Это часто включает в себя интеграцию передовых вычислительных возможностей с различными устройствами Интернета вещей (IoT), такими как датчики.

5Gconnectivity и edgecomputing идут рука об руку: сети 5G переносят компьютерную обработку (обычно размещенную в облаке) ближе к краю, где данные генерируются, анализируются и обрабатываются. Край может быть расположен в любом месте, в том числе

на территории предприятия. Вместе, 5G подключение, компактная вычислительная мощность и искусственный интеллект объединяются, чтобы создать интеллектуальный край, универсальную основу для раскрытия полного потенциала IoT и Industry 4.0.

По данным ABIResearch, синхронизация пограничных серверов с телекоммуникационной инфраструктурой представляет собой возможность в размере 54 миллиардов долларов к 2024 году. Кроме того, InternetDatabaseConnector прогнозирует, что через два года 45% данных, генерируемых IoT, будут храниться, обрабатываться, анализироваться и обрабатываться вблизи или на границе сетей. Позволяя агрегировать и обрабатывать данные на границе, компании могут добиться экономии пропускной способности, а также снижения задержки и повышения надежности.

Ключевые проблемы, которые необходимо преодолеть

На стороне предприятия телекоммуникационные провайдеры должны решить дилемму с точки зрения интеллектуального преимущества. В то время как некоторые провайдеры считают, что они могут получать больше дохода, сотрудничая с интернет—гигантами, другие опасаются, что их роль будет ограничена ролью партнера по подключению-фактически, действуя просто как ступенька для гиперскалеров и облачных гигантов. Поставщики понимают, что они должны действовать быстро, либо интегрируясь вертикально, либо используя горизонтальные возможности. Одна из их задач-определить, как построить свою текущую бизнес-структуру так, чтобы они оказались на месте водителя. Телекоммуникационные провайдеры также сталкиваются с возросшей конкуренцией со стороны поставщиков промышленных решений, таких как Bosch и Siemens, которые разрабатывают собственные пограничные сервисы.

Еще одна проблема связана со значительными затратами на эксплуатацию 5G. Многие провайдеры обеспокоены не только крутыми авансовыми инвестициями в строительство сети 5G, но и временным горизонтом, необходимым для реализации отдачи от своих инвестиций. С правительствами, требующими более высоких цен на 5G спектр, поставщики услуг могут быть оставлены без выбора, кроме как позволить потребителям платить за все или большую часть этого.

Самая большая забота руководителей сетей в связи с внедрением передовых беспроводных технологий-это безопасность. Высокая пропускная способность и повышенная скорость предоставляют хакерам еще больше возможностей для манипулирования сетью. Устройства, использующие технологию 5G, потенциально могут обойти платформы кибербезопасности, работающие по технологии 4G, предоставляя киберпреступникам платформу для запуска кибератак.

Наконец, из-за снижения трафика в магазинах из-за пандемии онлайн-интерфейсы стали неотъемлемой частью потребительского путешествия для телекоммуникационных провайдеров. Поэтому очень важно, чтобы телекоммуникационные компании предлагали как можно больше точек соприкосновения, чтобы улучшить качество обслуживания и удовлетворенность клиентов. Что касается опыта работы в магазине, телекоммуникационные провайдеры должны изучить, как технологии, обеспечивающие большую безопасность (например, «бесконтактные» среды), могут быть связаны с программами вознаграждений, возможностями привлечения потребителей и эксклюзивным опытом.

Действия, которые компании должны предпринять сейчас

- Сосредоточьтесь на преимуществах и результатах внедрения передовых беспроводных технологий, таких как 5G, а не на самой технологии.
- Используйте передовые беспроводные технологии, такие как 5G, для разработки корпоративных приложений, которые действительно являются отраслевыми.
- Развивайте лучшее понимание моделей использования клиентов с прицелом на укрепление ценностного предложения.
- Переоцените способы взаимодействия клиентов с бизнесом, уделяя особое внимание как сочетанию каналов, так и способности удовлетворять потребности клиентов (например, предлагая «бесконтактные» инвентаризации и проверки).

Стратегические вопросы для рассмотрения

● Должны ли мы капитализировать текущий акцент корпоративного клиента на безопасное, высококачественное подключение, чтобы ускорить внедрение новых продуктов и услуг, таких как 5G, Wi-Fi 6 и edgecomputing?

● Есть ли у нас достаточные возможности для управления значительным переходом клиентов на цифровые модели обслуживания и поддержки клиентов?

● Есть ли возможность укрепить и продвигать более дешевые, самообслуживаемые онлайн-продажи и каналы обслуживания клиентов? Как мы поощряем наших клиентов обращаться сначала к более дешевым цифровым каналам?

● Какие формы подключения и какие типы данных и приложений используют клиенты? Можем ли мы использовать эту информацию для понимания сетевых ограничений и соответствующего распределения будущих инвестиций?

ОБЕСПЕЧЕНИЕ ЦЕЛОСТНОСТИ, КОНФИДЕНЦИАЛЬНОСТИ ПЛАТЕЖНЫХ ДОКУМЕНТОВ ПРИ ОСУЩЕСТВЛЕНИИ ЭЛЕКТРОННЫХ РАСЧЕТОВ ЧЕРЕЗ ПЛАТЕЖНУЮ СИСТЕМУ БАНКА РОССИИ

Гвозденко Фёдор Денисович, курсант 1-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

С момента поступления ЭПД в платежную систему, Банк России возлагает на себя следующие юридически оформленные обязательства:
• обеспечение целостности и конфиденциальности электронного платежного документа;
• обеспечение правомерности списания и зачисления денежных средств.

Риски, связанные с возможной реализацией угрозы, по искажению реквизитов электронного платежного документа, в результате злонамеренных или ошибочных действий персонала БР, осуществляющего обработку платежных документов трудно недооценить. Достаточно «подправить» всего один платеж из потока денежных средств проходящих через систему электронных расчетов и кредитная организация может остаться без ликвидности, а районная больница без бюджетного финансирования.

Что же произойдет при осуществлении данного рода угрозы?
Во-первых, это прямые денежные потери клиента Банка России - при этом стоимость потерь равна сумме платежного документа. Во-вторых, это потеря имиджа Банка России как гаранта обеспечения стабильности платежной системы.

Какие предпринять действия, чтобы минимизировать риски реализации вышеописанных угроз?
Ответ на этот вопрос очевиден - необходимо реализовать эффективный механизм защиты платежной информации от преднамеренных или ошибочных искажений во время их обработки в платежной системе Банка России.

Основным инструментом, применяемым для обеспечения целостности платежных документов в электронной форме является ЭП. Кроме обеспечения целостности, ЭП несет в себе функцию аутентичности, которая позволяет достоверно определить автора электронного документа – лицо ответственное за его содержание.

Юридически использование ЭП для обеспечения целостности и аутентичности ЭД закреплено в договоре между клиентом - участником системы электронных расчетов и УБР, предоставляющим сервисы электронных расчетов. Исходя из договорных отношений, стороны признают юридическую силу ЭПД, подписанных ЭП (при положительном результате проверки ЭП), равной юридической силе документов на бумажном носителе, оформленных в соответствии с требованиями законодательства.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ В БЕСПРОВОДНЫХ СЕТЯХ

Гель Ангелина Владимировна, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Беспроводные сети становятся все более важным ресурсом в контексте развития корпоративных и домашних технологий. Одной из основных потребностей их использования является расширение существующих проводных сетей с минимальными затратами в кратчайшие сроки.

По мере увеличения числа мобильных пользователей возникает необходимость в кратчайшие сроки создавать между ними коммуникационные сети: обмениваться данными, получать информацию в кратчайшие сроки.

Поэтому, естественно, происходит бурное развитие беспроводных технологий. Поэтому возникает острая необходимость в защите таких сетей, обеспечении их информационной целостности и безопасности.

Несмотря на то, что тема безопасности беспроводных сетей поднимается из года в год, администраторы этих сетей часто забывают или пренебрегают простейшими мерами безопасности, и большинство устройств по-прежнему предоставляют большие возможности для хакеров.

С ростом вычислительной мощности пользовательского оборудования протоколы безопасности, разработанные несколько лет назад, быстро теряют свою актуальность.

Кроме того, вопрос физической безопасности в беспроводных технологиях выходит на новый уровень. Из-за отсутствия кабелей невозможно четко описать периметр защищаемой сети. Поэтому гораздо сложнее провести различие между авторизованными и неавторизованными пользователями.

С ростом популярности беспроводных сетей и идей умного дома беспроводные технологии часто используются для повышения уровня комфорта и объединения всех систем в единую сеть с единым центром управления, и одним из главных вопросов является обеспечение безопасности таких сетей, так как это начинает влиять на жизнь и здоровье человека, а не только на безопасность данных.

Таким образом, аспекты безопасности актуальны даже для беспроводных сетей, которые не имеют доступа к Интернету, но передают персональные данные или информацию, составляющую коммерческую тайну.

Список использованных источников

1.Бабин С. А. Лаборатория хакера. - СПб.: БХВ-Петербург, 2016. — 240 с.

2.Бирюков А.А. Информационная безопасность. Защита и нападение. – 2-е изд., перераб. и доп. – М.: ДМК Пресс, 2017. – 434 с

3.Пахомова А.С., Пахомов А.П., Юрасов В.Г., Обиспользовании классификации известных компьютерных атак в интересах разработки структурной модели компьютерной разведки / А.С. Пахомова, О.А. Остапенко // Информация и безопасность. – 2013. – Т. 16 № 3. – С. 115-118.

4.Аналитический обзор. – ZECURION ANALYTICS. Кибервойны 2017: Баланс сил в мире – 2017. – 7 с.

5.Alex WebKnacKer. Быстро и легко. Хакинг и антихакинг: защита и нападение. Учебное пособие. — М.: Лучшие книги, 2004 — 400 с.

ОБЪЕКТЫ ЗАЩИТЫ В КОНЦЕПЦИЯХ ИБ

Глазков Григорий Алексеевич, курсант 902 учебного взвода МосУ МВД им. В.Я. Кикотя рядовой полиции

Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Различие в субъектах порождает различия в объектах защиты. Основные группы объектов защиты:

- информационные ресурсы всех видов (под ресурсом понимается материальный объект: жесткий диск, иной носитель, документ с данными и реквизитами, которые помогают его идентифицировать и отнести к определенной группе субъектов);
- права граждан, организаций и государства на доступ к информации, возможность получить ее в рамках закона; доступ может быть ограничен только нормативно-правовыми актами, недопустима организация любых барьеров, нарушающих права человека;
- система создания, использования и распространения данных (системы и технологии, архивы, библиотеки, нормативные документы);
- система формирования общественного сознания (СМИ, интернет-ресурсы, социальные институты, образовательные учреждения).

Каждый объект предполагает особую систему мер защиты от угроз ИБ и общественному порядку. Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта.

ХАКЕРСКИЕ АТАКИ И ИХ ВИДЫ

Гордеева Полина Владимировна курсант 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Инциденты информационной безопасности по всему миру случаются очень часто, однако выявить их удаётся не сразу.

Хакерская атака – это комплекс действий, направленных на поиск уязвимостей в цифровых системах, например на компьютерах, смартфонах, планшетных устройствах или даже целых компьютерных сетях. Под хакерской атакой в настоящее время понимается «Покушение на систему безопасности», и склоняется скорее к смыслу следующего термина Крэкерская атака. Это произошло из-за искажения смысла самого слова «хакер».

Многие думают, что типичный хакер представляет собой талантливого молодого программиста-самоучку, способного специальным образом модифицировать аппаратное или программное обеспечение, для использования его в целях, первоначально не заложенных производителем. Но такой подход лишь упрощает взгляд на проблему и не позволяет осознать все многообразие мотивов, которые побуждают хакеров к действиям.

Крэкерская атака — действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании.

Сегодня термин «хакерство» обычно употребляется в контексте противоправных действий, а хакерами называют киберпреступников, которые стремятся получить финансовую выгоду, выразить протест, собрать определенную информацию (то есть занимаются кибершпионажем) или просто хотят развлечься.

Хакерские атаки обычно имеют технический характер (как, например, вредоносная реклама, которая внедряет на компьютер опасные объекты в теневом режиме и не требует участия пользователя). Однако хакеры также могут прибегать к психологическим методам, чтобы обманным путем заставить пользователя открыть вредоносное вложение или предоставить конфиденциальные данные. Такие методы называют методами социальной инженерии. Социальная инженерия - это описание методов, которые злоумышленники используют, чтобы заставить жертв нарушить протокол безопасности или отказаться от личной информации. Есть много тактик, которые ведут к этой цели, и они полагаются на психологические манипуляции, такие как соблазнение жертв, играя на их жадности, тщеславии или их готовности помочь кому-то.

«Хакерство» – это общий термин, обозначающий деятельность подавляющего большинства вредоносных объектов, а также кибератаки на компьютеры частных лиц, предприятий и государственных учреждений. Помимо социальной инженерии и распространения вредоносной рекламы, к часто используемым хакерским методам относятся:

- Ботнеты
- Переполнение буфера
- Программы-угонщики браузеров
- DDoS-атаки
- Программы-вымогатели
- Руткиты
- Троянские программы

- Вирусы
- Сетевые черви
- IP-спуфинг и другие.

Рассмотрим некоторые из них.

Переполнение буфера.

Это, возможно, один из самых распространенных типов атак в Интернете. Принцип данной атаки построен на использовании программных ошибок, позволяющих вызвать нарушение границ памяти и аварийно завершить работу Если программа работает под учётной записью администратора системы, то данная атака позволит получить полный контроль над компьютером жертвы, поэтому рекомендуется работать под учётной записью рядового пользователя, имеющего ограниченные права на системе, а под учётной записью администратора системы выполнять только операции, требующие административные права.

DDoS-атаки

Распределенная атака отказа в обслуживании (DDoS) - это сетевая атака, в которой субъекты угроз заставляют многочисленные системы (обычно зараженные вредоносными программами) отправлять запросы на определенный веб-сервер, чтобы разбить, отвлечь или нарушить его достаточно, чтобы пользователи не могли подключиться к нему. DDoS, или распределенные Отказ в обслуживании, который представляет собой вредоносную сетевую атаку, в которой участвуют хакеры, заставляющие многочисленные интернет-соединения подключаться устройства для отправки сетевых запросов связи на один конкретный сервис или веб-сайт с намерением подавляющего это с ложным трафиком или запросами. Это имеет эффект связывания всех доступных ресурсов для решения этих проблем запросов, а также сбой веб-сервера или отвлечение его достаточно, чтобы обычные пользователи не могли создать соединение между свои системы и сервер.

Чтобы осуществить DDoS-атаку, хакерам нужна армия зомби-компьютеров, чтобы выполнить их требования. Хакеры используют то, что мы называем а DDoSToolчтобы поработить компьютеры и построить свою армию. Это зомби-сеть ботов (ботнет) общаться сервер команд и управления (C&C), ожидающий команды от хакера, который запускает ботнет. В случае из DDoS-атаки может случиться, что десятки тысяч или даже миллионы ботов работают одновременно, чтобы отправить большие объемы сетевого трафика в направлении целевого сервера. Обычно, но не всегда, оригинальное заражение DDoSTool не пытается украсть данные или иным образом повредить хост. Вместо этого он лежит в спячке, пока его не призовут участвуйте в DDoS-атаке.

Мотивы, стоящие за атакой на веб-сайт или услугу, различаются. Активисты будут использовать DDoS, чтобы сделать политическое заявление против организации или правительства. Есть преступники, которые делают это, чтобы держать коммерческий сайт в заложниках, пока они получите выкупную выплату. Недобросовестные конкуренты использовали DDoS для грязной игры против конкурирующих компаний. Иногда DDoS-это еще и стратегия отвлечения внимания администраторов сайта, позволяющая злоумышленнику подбросить другое вредоносное ПО такие как adware, spyware,вымогателей, или даже унаследованный вирус .

Программы-вымогатели

Вымогательство вредоносных программ, или вымогателей, является тип вредоносного ПО, которое не позволяет пользователям получить доступ к своей системе или личным файлам и требует оплаты выкупа в приказываю восстановить доступ. Самые ранние варианты вымогателей были разработаны в конце 1980-х годов, и оплата должна была быть отправлено по улиточной почте. Сегодня вымогатели авторы приказывают, чтобы оплата была отправлена с помощью криптовалюты или кредитной карты. Существует несколько различных способов, которыми вымогатели могут заразить ваш компьютер. Одним из самых распространенных методов на сегодняшний день является через вредоносный спам, или malspam, который является нежелательная почта, которая используется для доставки вредоносных программ. Электронная почта может включать в себя заминированные

вложения, такие как PDF-файлыили документы MicrosoftWord. Он также может содержать ссылки на вредоносные веб-сайты.

Malspam использует социальную инженерию для того, чтобы обмануть людей в открытии вложений или нажав на ссылки появившись как законный—будь то, казалось бы, от надежного учреждения или друга.Киберпреступники используют социальную инженерию в других типах атак вымогателей, таких как выдача себя за ФБР с целью напугайте пользователей, чтобы заплатить им сумму денег, чтобы разблокировать их файлы.

Еще одним популярным методом заражения, достигшим своего пика в 2016 году, является мальвертизация.Malvertising, или вредоносная реклама, является использование интернет-рекламы, чтобы распространяйте вредоносные программы, не требуя почти никакого взаимодействия с пользователем. Во время просмотра веб-страниц, даже законных сайтов, пользователи могут быть направлены на криминальные серверы, даже не нажимая на рекламу. Сведения каталога этих серверов о компании компьютеры-жертвы и их расположение, а затем выберите вредоносное ПО, которое лучше всего подходит для доставки. Часто, что вредоносные программы это вымогатели.

Malvertising часто использует зараженный iframe, или невидимый элемент веб-страницы, чтобы сделать свою работу. Iframe перенаправляется на целевую страницу эксплойта, и вредоносный код атакует систему с целевой страницы с помощью набора эксплойтов. Все это происходит без ведома пользователя ,поэтому его часто называют загрузкой на диске.

Угонщики браузеров

Угонщик браузера - тип вредоносного ПО, которое овладевает контролем над настройками пользовательского браузера и автоматически перенаправляет на сайты, которые пользователь не намеревался посетить.Большинство угонщиков браузеров устанавливаются на компьютер под видом подключаемых модулей, более известных как расширения для браузеров или тулбары. Зачастую эти модули призваны повысить удобство просмотра интернет-страниц с помощью интерактивных компонентов, например, анимаций. Однако некоторые из них могут привести к тому, что ваш компьютер перестанет реагировать или будет отображать всплывающие сообщения и другое нежелательное содержимое.

IP-спуфинг

Тоже распространенный вид атаки в недостаточно защищённых сетях, когда злоумышленник выдает себя за санкционированного пользователя, находясь в самой организации, или же за её пределами. Для этого хакеру необходимо воспользоваться IP-адресом, который разрешён в системе безопасности сети. Такая атака возможна, если система безопасности позволяет идентификацию пользователя только по IP-адресу и не требует дополнительных подтверждений

Таким образом, любая атака представляет собой не что иное, как попытку использовать несовершенства системы безопасности жертвы либо для получения информации, либо для нанесения вреда системе в корыстных целях, поэтому причиной любой удачной атаки является профессионализм хакера и ценность информации, а так же недостаточная компетенция администратора системы безопасности в частности, несовершенство программного обеспечения, и недостаточное внимание к вопросам безопасности в компании в принципе.

РАЗРАБОТКА МЕТОДИКИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

Горичева Светлана Дмитриевна, курсант МосУ МВД России
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В целях обеспечения защиты прав и свобод человека и гражданина Российской Федерации при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, 27 июля 2006 года был принят федеральный закон №152-ФЗ «О персональных данных», регулирующий отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, не входящими в систему органов местного самоуправления муниципальными органами, юридическими лицами, физическими лицами с использованием средств автоматизации или без использования таких средств, если обработка персональных данных без использования таких средств соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации."

Однако нельзя говорить, что лишь многочисленные факты кражи персональных данных в государственных и коммерческих структурах являлись причиной принятия этого закона. "Существует и другая, не менее важная причина: в 2001 году Российская Федерация присоединилась к Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных. "Принятие этой конвенции является одним из требований, которые необходимо выполнить для вступления во Всемирную торговую организацию. К 2006 году эта Конвенция ратифицирована не была и содержащиеся в ней требования выполнены не были. К числу таких требований относилось, во-первых, принятие законодательства, которое охраняло бы персональные данные в соответствии с положениями Конвенции и, во-вторых, должен был быть создан государственный уполномоченный орган, который занимался бы защитой персональных данных российских граждан.

Казалось бы, мы должны только приветствовать появление закона, направленного на реализацию конституционных прав, на неприкосновенность частной жизни граждан, обязывающего всех тех, кто собирает наши данные, защищать их, как того требует закон.

Любая организация, обрабатывающая персональные данные своих сотрудников в отделе кадров, подготавливающая для органов налогового учета информацию о доходах, работающая с клиентскими базами, содержащими телефоны и адреса, в том числе для привлечения новых партнеров и заказчиков, поддерживающая программы лояльности для своих клиентов, в соответствии с действующим законодательством не позднее 1 января 2010 года должна защитить свои информационные системы персональных данных. "При этом лица, виновные в нарушении требований федерального закона «О персональных данных», несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность."

Государственный контроль и надзор за обработкой персональных данных в рамках своих полномочий осуществляют Роскомнадзор, ФСБ и ФСТЭК. Проверки могут быть как плановыми, так и на основании жалоб от субъектов персональных данных. Поэтому отсутствие организации в опубликованном плане проверок на конкретный год еще не означает, что эта организация не будет проверена в этом году.

Явные риски для бизнеса (штрафы, ущерб репутации, административное приостановление деятельности и пр.) не могут остаться незамеченными. Ни один игрок на рынке информационной безопасности не желает остаться в стороне, на организации сыпется шквал предложений по организации защиты персональных данных в соответствии с законодательством Российской Федерации. Стоимость предлагаемых проектов высока, а эффективность большинства из них вызывает сомнения: во-первых даже представители "федеральных органов исполнительной власти, осуществляющих контроль и надзор за" обработкой персональных данных неофициально признают несовершенство законодательства, но отказываются давать официальные разъяснения по отдельным вопросам, а во-вторых предлагаемые решения чаще всего не учитывают сформировавшуюся «внутреннюю культуру» организации, ее бизнес процессы и потребности, не адаптируются под конкретного клиента.

АВТОМАТИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ И ПОДДЕРЖАНИЯ УРОВНЯ ЖИДКОСТИ В ПРИЕМНОМ РЕЗЕРВУАРЕ КНС №1 МУП «ВОДОКАНАЛ»,Г.СТАРЫЙ ОСКОЛ

Грачева Римма Александровна, студентка 2-го курса
Научный руководитель Грачёва Алина Валентиновна, преподаватель высшей категории
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Автоматизация действующего оборудования подразумевает собой внесение изменений и усовершенствований, повышающих его технический уровень и эксплуатационные параметры — производительность, долговечность и точность, безопасность работы, легкость обслуживания.

Современные системы водоснабжения и канализации – это совокупность сложных сооружений, механизмов и аппаратов, все части которой должны точно и без сбоев работать совместно.

Разработка автоматизированной системы управления поддержания уровня жидкости в приемном резервуаре КНС №1 МУП «Водоканал» даст возможность снижения затрат электроэнергии, повышения качества и надежности подачи воды потребителям.

Целью данной работы являетсяразработка автоматизированной системы управления поддержания уровня жидкости в приемном резервуаре КНС №1 МУП «Водоканал», г. Старый Оскол.

Задача:

- разработка системы подержания уровня в объекте,
- выбор системного, информационного, технического и программного обеспечения
- обоснование внедрения системы автоматизации.

Объект исследованияКНС №1 МУП «Водоканал», г. Старый Оскол

Предмет исследования автоматизированная система управления поддержания уровня жидкости в приемном резервуаре.

МУП Водоканал – муниципальное предприятие обеспечивающие безопасную и комфортную жизнедеятельность города.

Предметом деятельности МУП «Водоканал» является:

- откачка (добыча) пресной воды;
-аккумулирование водных запасов, с их последующей очисткой и распределением;
- использование оборудования водно-канализационных систем;
- отведение отходов и сточных вод;
- сбор очищенных вод на специальных объектах;
-химический анализ и контроль, как исходных, так и очищенных вод, на всех ступенях обработки воды.

Отработанная вода подает в сточный коллектор и самотеком на канализационные насосные станции. КНС включает в себя комплекс гидротехнического оборудования и сооружений. Используются для перекачки промышленных и хозяйственно-бытовых сточных вод. Включает в себя грабельное отделение, приемное отделение и машинный зал. В грабельном отделении осуществляется грубая очистка от крупных предметов- бутылок, пакетов, веток и др. Специальная наклонная решетка, именуемая граблями, является фильтрующим элементом. Это делает консистенцию сточных вод более однородной, облегчая их откачку и подачу на другие сооружения, входящие в канализационную систему, для дальнейшей переработки и более тонкой очистки.

Дальше сточные воды поступают в приемный резервуар. В машинном зале на находятся насосы, которые по двум коллекторам обеспечивающие откачку из приемного резервуара на очистные сооружения.Очистные сооружения – это набор технологического оборудования, которое позволяет очищать сточные воды до необходимых нормативных показателей.

Канализационная насосная станция №1 МУП «Водоканал» предназначена для перекачки хозяйственно-бытовых и близких к ним по составу производственных вод, имеющих нейтральную или слабощелочную реакцию, и служит для перекачки сточных вод на очистные сооружения. На рисунке 1 представлена технологическая схема КНС.

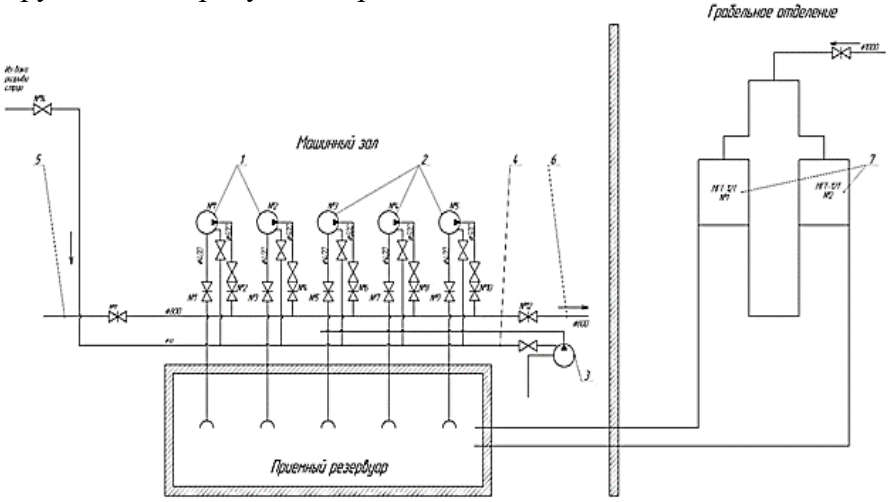


Рисунок 1 - Технологическая схема КНС

Технологическая схема включает в себя следующее оборудование:

1. Насос ФГ_540/95.
2. Насос СД – 2400/75.
3. Дренажный насос К90/55.
4. Трубопровод
5. Напорный трубопровод (левая нитка)
6. Напорный трубопровод (правая нитка)
7. Грабли механические МГ – 12Т

На КНС №1 автоматизация отсутствует.

Оператор вручную осуществляет полный объем процесса откачки сточных вод.

Датчик уровня не установлен в приемном резервуаре закрытого типа.

Оператор визуально, через технологические окна в грабельном отделении, осуществляет контроль уровня сточных вод.

Оператор вручную осуществляет регулирование, пуск и остановку производительности насосных агрегатов.

Автоматическое аварийное обесточивание насосных агрегатов установлено и безупречно функционирует.

Регулировка производительности насосного агрегата осуществляется посредством дросселирования напорного участка трубопровода.

Регулирование осуществляется электрифицированными задвижками.

В непосредственной близости от исполнительного механизма находятся кнопки управления приводом задвижки.

Положение открытия-закрытия задвижки оператор определяет визуально.

Выполнение операций по регулированию и управлению работы насосным агрегатом оператор руководствуется визуальным осмотром процесса.

Постановка задачи на разработку АСУТП. Разрабатываемая система автоматизации КНС 1 должна осуществлять работу круглосуточно, визуализировать тех процесс, управлять

насосными агрегатами, архивировать основные параметры тех процесса, выдавать регистрировать аварийные сообщения, передавать и получать информацию на единый диспетчерский пункт.

Чтобы решить проблему необходимо обеспечить автоматический контроль и мониторинг технологического процесса. Рекомендуется установить контроллер ОВЕН, разработать SCADA систему.

Также рекомендуется установить датчик уровня, аварийные датчики

Разрабатываемая модель системы автоматического регулирования имеет в себе два контура регулирования: контур регулирования уровня и контур регулирования расхода жидкости.

Задание по уровню Y*(t) в емкости сравнивается с текущим значением уровня Y(t), полученными с помощью датчика уровня. Сравнив сигналы, рассчитываем рассогласование, вычитая из текущего значения уровня заданное. После чего сигнал рассогласования поступает в ПИ регулятор. ПИ регулятор формирует значение угла поворота задвижки. Блок ограничения, ограничивает задание по углу поворота в необходимых пределах от 0 до 100 процентов. Задание по углу поворота сравнивается с текущим, полученным от датчика положения. Трехпозиционное реле формирует на основе рассогласования на исполнительный механизм формирует управляющий сигнал. От исполнительного механизма на вход модели объекта управления поступает управляющее воздействие. Кроме управляющего воздействия на поведение объекта управления влияет внешнее возмущение. Функция ПИ регулятора – обеспечить изменение угла поворота задвижки для увеличения откачки под влиянием внешнего возмущения [2].

На рисунке 2 представлена разработанная структурная схема системы подержания уровня в приемном резервуаре.

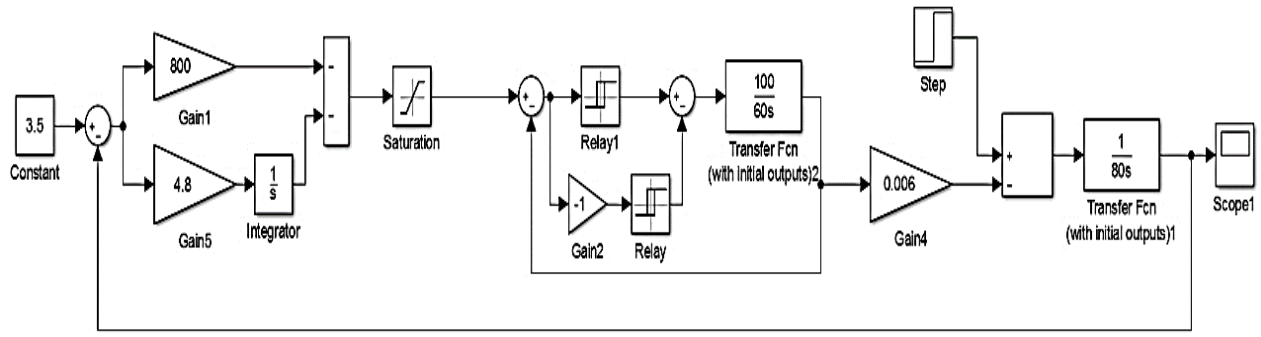


Рисунок 2 - Структурная схема системы подержания уровня в приемном резервуаре

Смоделируем работу системы. Блоком генератора ступенчатого сигнала Step используется в качестве внешнего возмущения- время наступления перепада сигнала 1000 сек.

Смоделируем систему регулирования в программной среде MatlabSimulink.

Результат моделирования представлен на рисунке 3.

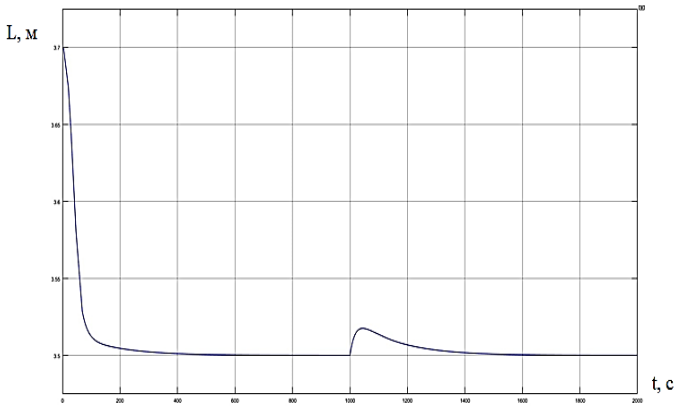


Рисунок 3- График работы системы и влияние внешнего возмущение

Система выходит на задание за 400 секунд без перерегулирования и статической ошибки. ПИ регулятор с подобранными коэффициентами обеспечивает необходимые требования к переходному процессу. Полученный переходный процесс показывает, что система справляется с резкими скачками уровня, что очень важно для безаварийной работы данного объекта. Время переходного процесса составило 400 секунд. Перерегулирование, статическая ошибка и колебательность отсутствуют. Система удовлетворяет требованиям.

Для реализации разрабатываемой системы выбрано следующее техническое обеспечение: контролер ОВЕН ПЛК160;модуль аналогового ввода МВ210;сетевой шлюзПВ210; ультразвуковой уровнемер МПУ-8;панель оператора СП307-Б;электропривод ГЗ-ОФ 630/30;датчик уровня ОВЕН ДУ;программное обеспечение контроллера CODESYS V.2.

Система обеспечит необходимые требования к качеству переходного процесса без ошибок.

Внедрение спроектированной системы позволит осуществлять работу круглосуточно, визуализировать тех процесс, управлять насосными агрегатами, архивировать основные параметры тех процесса, выдавать регистрировать аварийные сообщения, передавать и получать информацию на единый диспетчерский пункт, а так же позволит достичь положительного экономического эффекта за счет экономии на электроэнергии и оптимизации штата дежурного операторского персонала.

В экономической части работы произведен расчет экономической эффективности внедрения АСУ КНС. Капитальные затраты составили 588902 рубля. С точки зрения экономических расчетов внедрение АСУ подержания уровня дикости в приёмном резервуаре целесообразно, окупаемость вложений на приобретение, монтаж и внедрение технического обеспечения, наступает через 14. месяцев успешного функционирования системы.

Список использованных источников

1 Афонин А.М. Теоретичекие основы разработки и моделирования систем автоматизации: /учебное пособие А.М. Афонин, Ю.Н. Царегородцев - М.: Форум, НИЦ ИНФРА-М, 2016. - 105 с.

2 Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник / И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

3 Дозорцев В.М., Ицкович Э.Л., Кнеллер Д.В. Усовершенствованное управление технологическими процессами (АРС): 10 лет в России // Автоматизация в промышленности. –

2016. - №1. – с.12-19.
4 Евдокимов А.Г., Коринько И.В., Кузнецов В.Н., Ярошенко Ю.В. Трубопроводные транспортные системы. Теория. Практические приложения. Математические основы. Учебное пособие для вузов. – Харьков: издательство «Точка», 2017 г.

УПРАВЛЕНИЕ ИССЛЕДОВАТЕЛЬСКОЙ ДЕЯТЕЛЬНОСТЬЮ СТУДЕНТОВ В СТРУКТУРЕ МЕНЕДЖМЕНТА КОЛЛЕДЖА

Григорьева Любовь Владимировна, аспирант 2-го курса
Научный руководитель Шаповалов Валерий Кириллович доктор педагогических наук, профессор, заведующий кафедрой «Теория и методика профессионального образования
Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет»,
г. Ставрополь,

Изменения последних лет в области российского профессионального образования ставят перед руководителями образовательных учреждений новые управленческие задачи. Одна из задач образовательного учреждения состоит в том, чтобы сократить период адаптации студентов к учебно-исследовательской и научной работе. Решение этой задачи возможно в том случае, если с первых дней пребывания в колледже студент будет активно участвовать в разнообразных формах научной работы, проводимых кафедрами (отделениями, методическими объединениями). Успешность и результативность такой адаптации наряду с другими факторами обусловлена созданием органов управления, которые призваны определить цель, задачи, основные направления научной деятельности, формы, методы и средства их реализации. Внутриколледжное управление системой учебно-исследовательской деятельности студентов должно скоординировать деятельность преподавателей и мастеров, работающих со студентами на одном курсе, руководителей производственных практик и представителей вуза, выступающих в качестве научных экспертов учебных исследований.

Внутриколледжное управление системой учебно-исследовательской деятельности студентов следует понимать как непрерывную последовательность действий, осуществляемых должностными лицами, органами управления, структурными подразделениями колледжа. Они призваны разработать и обеспечить стабильное функционирование и устойчивое развитие целостной совокупности содержания, методов и форм организации совместной деятельности преподавателей и студентов по овладению системой знаний, умений, процедур творческой деятельности, ценностных ориентаций, позволяющих корректно осуществлять учебное исследование.Специфика учебно-исследовательской деятельности студентов предполагает, что управление будет основано на следующих принципах: системном, деятельностном, квалиметрическом, синергетическом и принципе субъект-субъектных отношений.

Необходимым фактором функционирования системы управления учебно-исследовательской деятельностью студентов является видение связей между частями системы. Понятие «система» означает цельный, единый инструмент, в котором возможно выделить отдельные части. В управлении исследовательской деятельностью как системой важно видеть не только основные части системы, но и те связи и отношения, которые возникают, складываются или разрушаются между этими частями. Другими словами, какие компоненты системы выступают в качестве системообразующих, такова и перспектива развития связей и отношений системы. Наличие структуры составляет признак системы. Система интергративна, это объясняется тем, что каждый элемент обладает своими качествами и присущими ему свойствами, при их взаимодействии образуются новые связи, компоненты, которые не сводятся к прежним.

Устойчивость интегративного свойства определяется целостностью системы. В управлении важно помнить и о ее тесной и специфической связи с внешней средой, которая оказывает сильное воздействие.

Важно, чтобы процесс управления учебно-исследовательской деятельностью студентов был оптимальным и целостным, т.е. после выявления всех связей выбирались те из них, которые позволяют добиться поставленных целей. Целостность будет выступать внутренним единством системы управления учебно-исследовательской деятельностью

учащихся.

Деятельностный подход к управлению подразумевает, что процессы обучения и воспитания не сами по себе непосредственно развивают человека, а лишь тогда, когда они имеют активные формы и обладают соответствующим содержанием, в нашем случае в старшем школьном возрасте формируются те или иные умения, согласно ведущим типам деятельности. Следовательно, ориентируясь на ведущий тип деятельности старшеклассника, организация материала, предоставляющая ученику возможность выбора содержания, методов поиска и переработки учебных знаний, стимулирует развитие исследовательской направленности в деятельности учащихся.

Как уже отмечалось выше, для успешного ведения в колледжах и техникумах научно-исследовательской работы студентов преподаватель СПО должен представлять структуру научно-исследовательской деятельности студентов в условиях СПО, а также знать общие принципы ведения научной работы применительно к условиям своего труда.

В основу определения содержания функций внутриколледжного управления системой учебно-исследовательской деятельности студентов в условиях профессионального обучения нами положена точка зрения Ю.А. Конаржевского [1] и Т.И. Шамовой [2] на управленческий цикл, который представляет собой: анализ, планирование, организация, контроль, регулирование.

Структура управления согласно функциям, где управление разделено на функциональные службы, за каждой из которых закреплен определенный круг работ, в большей мере соответствует такому объекту как развитие исследовательской компетентности студентов, так как предполагает вовлечение в этот процесс значительного количества преподавателей и мастеров, создания и освоения нововведений, требующих компетентных решений, учитывающих мнение большинства членов педагогического коллектива. Это предполагает взаимную согласованность деятельности традиционных методических объединений преподавателей, структурных подразделений колледжа, обеспечивающих стабильность образовательного процесса, и временных групп преподавателей, инновационных органов управления, способствующих развитию образования, что обеспечивает достижение, с одной стороны, оперативности и простоты, а с другой – коллегиальности и компетентности внутриколледжного управления системой учебно-исследовательской деятельности студентов.

При организации и проведении научно-исследовательской деятельности определяются основополагающие принципы исследования:

- единство и активное взаимодействие научно-исследовательской, инновационнно-проектной и образовательной деятельности;
- направленность на социальное и духовное развитие личности;
- концентрация усилий и ресурсов на приоритетных, социально значимых и недостаточно освоенных направлениях;
- поддержка и развитие научного творчества обучающихся;
- поддержка ярких творческих индивидуальностей, способных обеспечить высокий уровень проводимых исследований;
- доведение результатов исследований и проектов до применения в практической деятельности, используя при этом издательскую деятельность и возможности сети Интернет;
- развитие многообразия форм организации научно-исследовательской и творческой деятельности.

Проблемы, с которыми приходится сталкиваться при организации НИРС:

1. Слабая ресурсная база (материально-техническая): уменьшение денежных средств на подписку, покупку литературы, лабораторного оборудования.

2. Отсутствие связи с работодателями, что затрудняет получение информации.

3. Недостаточная мотивация студентов и преподавателей.

4. Неотработанность новой системы оплаты труда педагогических работников в соответствии с задачами инновационного развития.

5. Слабая подготовленность студентов к научно-исследовательской работе.

Пути решения данных проблем следующие:

- ввести в учебный план спецкурс «Основы научно-исследовательской деятельности

студентов»;

- научно-исследовательская деятельность должна быть непрерывная, начиная с 1 курса и до окончания обучения;
- заниматься ею должны все преподаватели, и при этом необходимо учитывать её результаты при аттестации педагогических работников;
- за системность в работе требуется материально поощрять преподавателей;
- подбирать индивидуальные формы научно-исследовательской деятельности для каждого студента;
- осуществлять поиск спонсоров и социальных партнёров.

Масштабность и эффективность проектно-исследовательской деятельности студентов под руководством преподавателей во многом определяется ее моральным стимулированием и материальным вознаграждением.

Исследовательская компетенция считается метапредметной и включает в себя комплекс образовательных компетенций, напрямую связанных с мыслительными, поисковыми, логическими, творческими процессами познания студентов. В рамках освоения учебных дисциплин и профессиональных модулей формирование этой компетенции не может быть эффективно осуществлено. Необходимо введение внеаудиторной занятости в виде изучения курса или дисциплины.

Исследовательская деятельность имеет свои формы и методы. Она может носит аудиторный и внеаудиторный характер. Выполнение НИР представляет собой совокупность различных форм: работа в студенческих кружках, участие в исследованиях, проводимых студентами техникума; исследовательская работа, проводимая по индивидуальному плану; участие в научно-теоретических конференциях, выступления с докладами и сообщениями по материалам собственных исследований.

При формировании исследовательских навыков введения научно-исследовательской работы нужно понимать, что научно-исследовательской деятельностью должен заниматься каждый студент, это не должно носит характер выделения сильных обучающихся.

Внутриколледжное управление системой учебно-исследовательской деятельности студентов должно скоординировать деятельность преподавателей и мастеров, работающих со студентами на одном курсе, руководителей производственных практик и представителей вуза, выступающих в качестве научных экспертов учебных исследований.

Список использованных источников

1. Конаржевский Ю.А. Менеджмент и внутришкольное управление. – М.: Центр «Педагогический поиск», 1999. – 224 с.Шамова Т.И. Исследовательский подход в управлении школой. – М.: АПП ЦИТП, 1992. – 66 с
2. Шепелев М.В., Румянцев Е.В., Вашурин А.С. Организация научно-исследовательской деятельности учащихся в системе «Школа – вуз»: Опыт регионального университета. Известия высших учебных заведений. Гуманитарные науки, 2013, т. 4.№ 3, с. 210–214.
3. Широбокова Т.С. Организация и проведение исследовательской деятельности обучающихся в образовательных учреждениях системы СПО / Т.С. Широбокова // Научные исследования в образовании. – 2011. – № 7.
4. Шихова, А.Л. Организация исследовательской деятельности студентов колледжа / А.Л. Шихова //Сборник материалов по итогам областного студенческого форума: сб.ст./ под общ.ред. М.Ю. Козловой. – Киров: Изд-во ООО «Радуга-ПРЕСС», 2012.-114

ЦЕЛОСТНОСТЬ ДАННЫХ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Гуенок Василий Владимирович, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры
СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Целостность данных

Целостность, безопасность, разборчивость. Это относится к данным, будь то бумажным или электронным, и эти простые принципы должны быть частью ваших жизненных циклов данных, ВВП и инициатив по обеспечению целостности данных. Это помогает в разработке стратегий, обеспечивающих целостность доказательств, как в научных исследованиях, так и в производстве. Целостность информации — термин в информатике (криптографии, теории телекоммуникаций, теории информационной безопасности), означающий, что данные не были изменены при выполнении какой-либо операции над ними, будь то передача, хранение или отображение.

В телекоммуникации целостность данных часто проверяют, используя хеш-сумму сообщения, вычисленную алгоритмом MAC (англ. message authentication code).

В криптографии и информационной безопасности целостность данных (в широком смысле) — это сохранение данных в том виде, в каком они были созданы. Примеры нарушений целостности данных:

- попытка злоумышленника изменить номер аккаунта в банковской транзакции, или попытка подделки документа;
- случайное изменение информации при передаче или при неисправной работе жёсткого диска;
- искажение фактов средствами массовой информации с целью манипуляции общественным мнением.
- В теории баз данных целостность данных означает корректность данных и их непротиворечивость. Обычно она также включает целостность связей, которая исключает ошибки связей между первичным и вторичным ключом. Примеры нарушений целостности данных:
- существование записей-сирот (дочерних записей, не имеющих связи с родительскими записями);
- существование одинаковых первичных ключей.

Для проверки целостности данных в криптографии используются хеш-функции, например, MD5. Хеш-функция преобразует последовательность байт произвольного размера в последовательность байт фиксированного размера (число). Если данные изменятся, то и число, генерируемое хеш-функцией, тоже изменится.

Целостность данных — свойство, при выполнении которого данные сохраняют заранее определённый вид и качество. Это требует использования безопасных и уникальных пользовательских логинов и электронных подписей. Всегда следует избегать использования общих идентификаторов входа или совместного использования учетных данных. Уникальные входы в систему позволяют отдельным лицам связываться с созданием, изменением или удалением данных в записи. Должна быть возможность продемонстрировать, что эту функцию выполнял обученный и квалифицированный персонал. Это относится и к изменениям, внесенным в записи: исправления, удаления, изменения и т. Д.

Разборчивость: созданная запись, особенно бумажные записи, должна быть разборчивой. Записи должны быть постоянными и не стираемыми, чтобы они были надежными на протяжении всего жизненного цикла данных. Термины разборчивые,

отслеживаемые и постоянные относятся к требованиям, чтобы данные были читаемыми, понятными и позволяли получить четкое представление о последовательности шагов или событий в записи. Это очень важно в фармацевтической промышленности, так как ошибочное написание может привести к введению совершенно другого лекарства. Чтобы электронная запись считалась разборчивой, отслеживаемой и постоянной. Запретить создание данных во временной памяти, а также немедленную фиксацию данных в постоянной памяти, прежде чем двигаться дальше.

Одновременность - это свидетельство действий, событий или решений, которые должны регистрироваться по мере их возникновения или генерирования. Эта документация должна служить точным подтверждением того, что было сделано или что было решено и почему, т.е. что повлияло на решение в то время. Если выполняется протокол валидации, тесты должны быть выполнены и их результаты записываются так, как это происходит в утвержденном протоколе.

Оригинальность: исходные данные иногда называют исходными или первичными данными, независимо от того, записаны ли они на бумаге (статические) или в электронном виде. Информация, которая первоначально захвачена в динамическом состоянии, должна оставаться доступной в этом состоянии. Это может быть база данных, утвержденный протокол или форма, или специальный блокнот. Важно, чтобы ваши исходные данные были сгенерированы таким образом, чтобы их содержание и смысл сохранялись. Например: убедитесь, что результаты проверочного теста записаны в утвержденном протоколе. Запись результатов в тетрадь для последующей записи может привести к ошибкам, и если ваши исходные данные написаны от руки и должны храниться в электронном виде, убедитесь, что создана «истинная копия», копия проверена на полноту, а затем перенесена в электронную систему.

Точность: Записанные данные должны быть правильными, правдивыми, полными, достоверными, надежными, без ошибок и отражающими наблюдения. Редактирование не должно выполняться без документирования и аннотирования изменений. Например, если для сбора критических данных используются свидетельские показания. Видеозаписи процесса создания записей также получают признание в этом отношении. Эти стандарты гарантируют, что данные собираются и обрабатываются с целостностью.

Методы и способы реализации требований, изложенных в определениях термина, подробно описываются в рамках единой схемы обеспечения информационной безопасности объекта (защиты информации).

Основными методами обеспечения целостности информации (данных) при хранении в автоматизированных системах являются:

- обеспечение отказоустойчивости (резервирование, дублирование, зеркалирование оборудования и данных, например через использование RAID-массивов);
- обеспечение безопасного восстановления (резервное копирование и электронное архивирование информации).

Одним из действенных методов реализации требований целостности информации при её передаче по линиям связи является криптографическая защита информации (шифрование, хеширование, электронная цифровая подпись).

Шифрование данных не гарантирует того, что целостность данных не будет нарушена. Поэтому для проверки целостности данных в криптографии используются дополнительные методы. Под нарушениями целостности данных понимается следующее:

- инверсия битов;
- добавление новых битов (в частности совершенно новых данных) третьей стороной;
- удаление каких-либо битов данных;
- изменение порядка следования бит или групп бит.

В криптографии решение задачи целостности информации предполагает применение мер, позволяющих обнаруживать не столько случайные искажения информации, так как для

этой цели вполне подходят методы теории кодирования с обнаружением и исправлением ошибок, сколько целенаправленное изменение информации активным криптоаналитиком.

Процесс контроля целостности обеспечивается введением в передаваемую информацию избыточности. Это достигается добавлением к сообщению некоторой проверочной комбинации байт. Такая комбинация байт вычисляется согласно определённым алгоритмам и позволяет проверить, были ли данные изменены третьей стороной. Вероятность того, что данные были изменены, служит мерой имитостойкости шифра.

Дополнительную избыточную информацию, вносимую в сообщение, называют имитовставкой. Имитовставка может вычисляться до начала или во время шифрования сообщения.

Физическая целостность имеет дело с проблемами , связанными с правильно хранения и извлечения самих данных. Проблемы с физической целостностью могут включать в себя электромеханические недостатки, конструктивные недостатки, материалы усталости , коррозию , перебои в подачу электроэнергии, стихийные бедствия, акты войны и терроризм, а также другие специальные опасности для окружающей среды , таких как ионизирующее излучение, экстремальные температуры, давление и G-силу . Обеспечение физической целостности включает в себя такие методы, как с резервированием оборудования, с источником бесперебойного питания , некоторые типы RAID - массивов, радиационно - чипов, памяти с коррекцией ошибок , использование кластерной файловой системы , используя файловые системы , которые используют блок на уровне контрольных сумм , таких как ZFS , хранение массивы , которые вычисляют вычисление четности , такие как исключающие или или используют криптографические хэш - функцию и даже имеющие сторожевой таймер на критических подсистемах.

Физическая целостность часто делает широкое использование алгоритмов обнаружения ошибок , известных как помехоустойчивых кодов . Ошибки целостности данных , антропогенные часто обнаруживаются за счет использования более простых проверок и алгоритмов, таких как алгоритм Дамм или алгоритма Лун . Они используются для поддержания целостности данных после ручной транскрипции из одной компьютерной системы в другую, у человека посредникам (например , кредитной карты или банковского маршрутизации номеров). Компьютер-индуцированная ошибка транскрипции может быть обнаружена с помощью хэш - функции.

В производственных системах, эти методы используются вместе , чтобы обеспечить различную степень целостности данных. Например, компьютер файловая система может быть настроена на массив RAID отказоустойчивой, но не может обеспечить контрольные суммы на уровне блоков , чтобы обнаружить и предотвратить беззвучное искажение данных . В качестве другого примера, система управления базами данных может быть совместим с ACID свойствами, но контроллер RAID или внутренний кэш записи накопителя на жестком диске не может быть.

Логическая целостость

Этот тип целостности связан с правильностью или рациональностью куска данных, учитывая конкретный контекст. Это включает в себя такие темы, как ссылочную целостность и целостность сущностей в реляционной базе данных или правильно игнорируя невозможные данные датчика в роботизированных системах. Эти проблемы включают обеспечение того, чтобы данные «имеет смысл», учитывая его окружение. Проблемы включают в себя программные ошибки, ошибки проектирования, и человеческие ошибки. Общие методы обеспечения логической целостности включают в себя такие качества , как проверки ограничений , ограничений внешнего ключа , программные утверждения , и другие во время выполнения проверки вменяемости.

И физические и логическая целостность часто имеет много общих проблем, такие как человеческие ошибки и недостатки дизайна, и оба они должны надлежащим образом иметь дело с одновременными запросами для записи и извлечения данных, последние из которых является полностью предметом по себе.

Целостность данных содержит руководящие принципы для хранения данных , с указанием или гарантировать длительность временных данных может быть сохранена в конкретной базе данных. Для достижения целостности данных, эти правила последовательно и регулярно применяются ко всем данным , входящих в систему, и любое ослабление органов может привести к ошибкам в данных. Осуществление проверки на данных как можно ближе к источнику входного (например, ввод данных человека), в меньшей степени вызывает ошибочные данные для входа в систему. Строгое соблюдение целостности данных правил приводит к снижению частоты ошибок, а сэкономленное время устранения неисправностей и отслеживания ошибочными данные и ошибки , что вызывает к алгоритмам.

Целостность данных также включает в себя правила , определяющие отношения часть данных может иметь, к другим частям данных, такие как клиент запись разрешают ссылки на приобретенные продукты , но не несвязанные данных , такие как корпоративные активы . Целостность данных часто включает в себя проверку и исправление для недостоверных данных, основанных на фиксированной схеме или заранее определенного набора правил. Пример того текстовые данные , введенные где требуется значение даты и времени. Правила вывода данных также применимы, с указанием того, как значение данных выводятся на основе алгоритма, участник и условиях. Он также определяет условия о том , как значение данных может быть повторно получено.

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ТЕЛЕКОММУНИКАЦИОННОЙ КОМПАНИЕЙ С ИСПОЛЬЗОВАНИЕМ СБАЛАНСИРОВАННОЙ СИСТЕМЫ ПОКАЗАТЕЛЕЙ

ГунашевАбдулатипАхмедович, студент 1-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Каждый из нас сегодня является свидетелем стремительных изменений в качестве жизни вносимых технологическими изменениями. И в первую очередь, это технологическое преобразование общения, возведение самого определения понятия общения на качественно новый уровень понимания и восприятия. На рынке телекоммуникаций практически каждый день появляются как новые технические средства общения, так и все новые и новые технологии. И если еще не более десятилетия назад в авангарде телекоммуникационных технологий приоритетным направлением являлось развитие голосовых услуг связи, то сегодня с каждым днем на первый план выходят технологии обеспечения передачи и обработки восходящих потоков цифровой информации.

При появлении технологии беспроводного мобильного общения, так же стремительно образовался и рынок предоставления данных услуг. И на текущий момент, он естественным образом распределился между четырьмя основными игроками. В условиях такой тяжелой конкуренции (несмотря на небольшое количество основных игроков, они, в силу отраслевых особенностей имеют основные доли рынка) закономерно встает вопрос о стратегии и методах закрепления на данном рынке услуг, завоевания и увеличения своей «части пирога». Для этого необходим инструмент, который позволит выделить главные (ключевые) цели, укажет пути их достижения, позволит сделать участниками процесса достижения этих целей всех сотрудников компании. Инструмент, который позволит создать систему контроля ключевых показателей эффективности на пути реализации стратегии компании. Одну из основных стратегических целей можно сформулировать следующим образом: "Мы станем самыми эффективными имея максимально возможную долю рынка при имеющихся ресурсах, и иметь лучший возврат инвестиций в отрасли". Пути реализации данной стратегии, наверняка, видят инвесторы и генеральный директор, видят возможности её достижения. Однако встает вопрос об эффективном вовлечении в данные процессы ключевых сотрудников. Вопрос о подходах и методах достижения ключевых показателей эффективности, определенных в составе основных стратегических целей.

Цели работы:

Определение и описание существующей стратегии компании, ключевые показатели эффективности основных целей.

Описание классических методов построения и развития сети подвижной мобильной связи. Философия разумного вложения инвестиций SmartCAPEX. Описание и внедрение методологии распределения капитальных вложений на основе качественных показателей голосовых услуг и прогноза потерь выручки.

Оценка предполагаемого положительного эффекта от реализации новой методологии распределения капитальных вложений на один из ключевых показателей эффективности уже принятой стратегии развития компании «Лучший возврат инвестиций (ROIC)».

Основная задача:

На основе вышеописанного подхода, подвергнуть более детальному рассмотрению реализацию одного из ключевых показателей эффективности уже принятой стратегии

развития компании «Лучший возврат инвестиций (ROIC)» посредством внедрения новой методологии распределения капитальных вложений.

В результате

«Приземлить» новую методологию на существующую стратегию компании с привязкой к ключевым показателям эффективности (один из ключевых показателей эффективности уже принятой стратегии развития компании «Лучший возврат инвестиций (ROIC)»). Оценить предполагаемый положительный эффект от предложенных изменений.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Гусейнов Эмир Наврузович
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

1) Киберпреступников не интересуют компьютеры частных лиц

К счастью, этому высказыванию мало кто верит. В данном случае утверждение также ложно.

Разумеется, корпоративные сети интересуют киберпреступников, но их сложнее заразить. Сегодня частные компьютеры так же хорошо подходят в качестве составляющих ботсетей. К тому же очень часто на них хранится много интересных персональных данных, таких как данные доступа к онлайн-магазинам, социальным сетям и учетным записям электронной почты или данные о кредитных картах, из которых киберпреступники могут извлечь выгоду. Поэтому не стоит недооценивать значение частных компьютеров для злоумышленников.

2) Большинство вредоносных программ распространяется по электронной почте

Данный тезис устарел, но, несмотря на это, данной точки зрения придерживается 54% участников опроса. В конце прошлого тысячелетия рассылка вирусов Melissa и I love you по электронной почте стала наиболее популярным способом распространения вредоносных программ. Приблизительно шесть лет назад на смену отправке электронных сообщении с зараженными вложениями пришли сообщения со ссылками на файлы, размещенные на Web-сайтах. Данная тактика позволяла злоумышленникам обходить очень эффективные спам-фильтры и доставлять сообщения ничего не подозревающему пользователю. С другой стороны, многие пользователи стали очень осторожны с сообщениями от неизвестных отправителей и в лучшем случае сразу удаляют их, не открывая. В большинстве случаев ссылки в электронных сообщениях направляют на вредоносные Web-сайты. Таким образом, появляются дополнительные возможности для поиска жертв: например, социальные сети, оптимизация поисковых запросов, ошибочные домены и т.д. Вредоносные программы находятся на Web-сайтах, а Web-сайты являются вектором заражения номер один.

3) Заражение ПК не происходит при загрузке зараженного Web-сайта

То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов "попутной загрузки" возможно уже на протяжении многих лет. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке".Во-первых, Web-сайты, созданные специально с целью заражения ПК.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое заражение ПК вредоносной программой. Преимуществом данного способа для киберпреступников является то, что им не приходится рекламировать Web-сайт. Для дальнейшей манипуляции данным Web-сайтом злоумышленникам необходимо в него внедриться. Если Web-сайт хорошо защищен, то осуществить такое внедрение очень сложно.

4) Большинство вирусов и вредоносных программ распространяются посредством зараженных файлов на файлообменниках

Бесспорно, определенное количество вредоносных программ распространяется через такие системы обмена файлами, как торренты и одноранговые сети. Неудивительно, что 48% участников опроса считают, что данный способ является основным в распространении

вредоносного ПО. Наверняка тот или другой пользователь уже хотя бы раз заражал свои компьютер вирусом после посещения подобных сайтов. Однако данный тезис также ложен и является мифом, поскольку большинство вредоносных программ распространяется через вредоносные Web-сайты.

5) Мой брандмауэр защищает меня от заражения при "попутной загрузке"

Данному утверждению верит 26% опрашиваемых. Этот тезис ложен. Брандмауэры – это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной Web-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных задании вредоносной программой и, например, отправку данных злоумышленникам, если речь идет о шпионских программах.

6) Если не открывать зараженные файлы, то ПК нельзя заразить

Это высказывание основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно лишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открытия зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

7) Большинство вредоносных программ распространяется через USB-накопители

В последние годы популярность флешек и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. Поэтому настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя.

8) Я не посещаю странные Web-сайты, поэтому мне не угрожает заражение при "попутной загрузке"

Данное утверждение можно опровергнуть так же, как и шестой тезис. Тематика Web-сайта не играет для киберпреступников никакой роли. Они заинтересованы в том, чтобы с минимальными затратами заразить вредоносными кодами максимальное количество посетителей. Это удается злоумышленникам, помимо всего прочего, с помощью манипуляции с баннерами и постоянных атак крупных доменов. В случае успеха и получения доступа они внедряют вредоносный код с помощью так называемых эксплойт-инструментов, и специальные знания для этого не требуются. Web-саиты, которые на протяжении многих лет считались достойными доверия, могут быть взломанными и в результате таить в себе опасность заражения.

9) Обеспечение информационной безопасности в облачной инфраструктуре

При защите данных в публичном облаке, я выделяю два направления, так называемую безопасность облака, и безопасность в облаке. Безопасность в облаке обеспечивает провайдер, и мы на нее влиять никак не можем, поэтому здесь важно грамотно подойти к выбору поставщика облачных услуг и установлению с ним отношений. Для безопасности облака, в той части, где мы можем обеспечивать дополнительную безопасность, с помощью специальных программных средств и политик, сформулированы также свои рекомендации. Рассмотрены подходы к выбору облачного провайдера. Разработан ряд критериев по ИБ, которым должны соответствовать облачные провайдеры и на которые можно опираться при выборе поставщика облачных услуг.

Особое внимание уделено установлению партнерских отношений с провайдером, т.к. доверие к провайдеру и партнерские отношения исключительно важны, в том числе и для обеспечения ИБ

данных. Доверие провайдеру очень важный пункт, но лучше чтобы дружба была подкреплена грамотно заключенным договором о предоставлении услуг и соглашением об уровне обслуживания (SLA). Данные документы могут иметь решающее значение при возникновении спорных ситуаций, в том числе связанных с ответственностью в вопросах ИБ.

10) Целостность информации

Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ В ПРАВООХРАНИТЕЛЬНОЙ СФЕРЕ

Данилова Евгения Антоновна, студент 2-го курса.
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Государственная политика в сфере использования информационных технологий призвана обеспечить координацию деятельности федеральных органов государственной власти по созданию государственных информационных систем в интересах общественной безопасности, включая и совершенствование системы проведения оперативно-розыскной работы и криминалистической деятельности. В настоящее время в России цельные работы в сфере использования биометрии в правоприменение отсутствуют, а специальные исследования, которые рассматривают биометрию как раздел криминалистической науки, почти не проводилось.

Актуальность данной проблемы заключается в том, что для ее решения необходим комплексный анализ и специальное научное исследование теоретических конструкций систем биометрической идентификации, которые интерпретируются с точки зрения их соответствия правовой реальности и возможности прописать статус существования тем или иным используемым в теории криминалистической идентификации абстрактным объектам.

Для понимания данной темы, необходимо рассмотреть законодательство РФ о биометрии: ФЗ от 15 августа 1996 г. №114-ФЗ «О порядке выезда из Российской Федерации и въезда в Российскую Федерацию», там сообщалось, что паспорта граждан «могут содержать электронные носители информации с записанными на них персональными данными владельца паспорта, включая биометрические персональные данные».

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». Статья 11 «Биометрические персональные данные».

В 2007 году были введены в действие ГОСТ Р ИСО/МЭК 19795-1–2007 «Автоматическая идентификация. Идентификация биометрическая. Эксплуатационные испытания и протоколы испытаний в биометрии.

Также ГОСТ Р ИСО/МЭК 19794 - определяет требования ко всем основным биометрическим параметрам и к их измерению. Так, например, части 2-4, 8 касаются отпечатков пальцев, часть 5 — изображения лица, а часть 14 — данных ДНК.

После этого было принято Постановление Правительства Российской Федерации от 6 июля 2008 г. № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных».

После чего, 31 декабря 2017 года Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» пополнился статьей 14.1 «Применение информационных технологий в целях идентификации граждан Российской Федерации», которая составляет фундамент для единой биометрической системы (ЕБС) и ее применения, а также увязывает ее с единой системой идентификации и аутентификации.

Затем, Федеральный закон от 31 декабря 2017 г. № 482-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации». Он призван образовать фундамент для Единой биометрической системы, регламентировать связанные с ней процедуры и области ее применения.

Биометрические системы аутентификации — системы, которые используют для удостоверения личности людей применение биометрических способов идентификации. Они делятся на два класса:

- Статические методы биометрической идентификации основаны на физиологических характеристиках человека, которые сохраняются у человека всю жизнь, они не могут быть изменены или потеряны.
- Динамические методы биометрической идентификации основаны на характерных для подсознательных движений в процессе воспроизведения или повторения какого-либо обыденного действия.

Сейчас мы рассмотрим статические методы биометрической идентификации личности, т.к в настоящем времени данных метод является более надежным, чем динамический, который может измениться в течении времени или который можно изменить.

Идентификация по отпечатку пальца. Данный способ идентификации является наиболее простым в процедуре получения данных, так же из плюсов данного метода стоит ответить низкую стоимость оборудования позволяющая производить необходимые действия для сбора информации. Минусами данного метода является низкая защищенность от подделки.

Идентификация по радужной оболочке глаза. В настоящее время данный способ становиться все более популярным из-за того, что радужная оболочка имеет сложную структуру, поэтому даже не качественный снимок позволяет определить личность человека, так же, данный метод не изменяется в течение времени, конечно, есть шанс повреждения сетчатки глаза, но он менее вероятен, чем повреждения рук, ладонь, которые так же используют для биометрической идентификации. Главный минус – это высокая стоимость оборудования.

Идентификация по сетчатки глаза. В 2012 году ученые из США (Университет Нотр-Дам) обнаружили, что есть погрешности в определении личности людей, чьи данные были внесены в базу ранее, вследствие чего было доказано, что рисунок сетчатки может изменяться в течение жизни человека. Так же данный метод сложен в воспроизведение.

Идентификация по геометрии рук. Метод распознавания геометрии требует достаточно малого объема информации — всего 9 байт, что позволяет хранить большой объем записей, следовательно, быстро осуществлять поиск. Но также стоит отметить, что форма кисти руки достаточно сильно подвержена изменениям во времени. Идентификацию по геометрии рук часто сравнивают с идентификации по отпечатку пальца, поэтому стоит отметить, что аппаратура для снятия узора с руки занимает больше места, чем пальцев рук, что в итоге ведет к повышению цены оборудования.

Идентификация по геометрии лица. Система запоминает и опознает черты человеческого лицо, то есть: контуры носа, форму бровей, губ и расстояние между отдельными чертами. Однако, стоит отметить, что, процесс идентификации по геометрии лица — задача сложная, потому что на восприятие машины влияет внешние условия, такие как: освещение, макияжа, угол наклона головы. Так же стоит учитывать обстоятельства, при которых, может быть изменен облик человека, это может быть пластическая хирургия или изменения черт лица, после аварии.

Идентификация по термограмме лица. Главным минусов данного метода считается, что биометрический идентификатор, не будет абсолютно точно совпадать с идентификатором из базы данных т.к. сигнатура термограммы лица сильно зависит от эмоционального состояния испытуемого, температуры тела и т.д., так же стоит обратить внимание на высокую стоимость оборудования. Плюсами считается то, что инфракрасная камера имеет возможность захвата термограммы лица при очень низкой освещенности или при отсутствии света, так же термограмма лица уникальна для каждого человека.

В настоящее время основным способом идентификации личности является распознавание отпечатков пальцев, потому что: во многих странах начался переход на

паспорта с биометрическими данными; разработка обновленных моделей сканеров пальцевых отпечатков для применения в маленьких устройствах.

Существуют основные прогнозы, которые сводятся к тому, что внедрение биометрических устройств безопасности в скором будущем приобретет лавинный характер. Благодаря интенсивному развитию мультимедийных и цифровых технологий и дальнейшее их удешевление позволят разработать и внедрить принципиально новые системы идентификации.

Определенные биометрические технологии сейчас проходят стадию разработки и некоторые из них признаны перспективными: термограмма лица в инфракрасном диапазоне; характеристики ДНК; параметры походки человека; индивидуальные запахи человека; уровень солености кожи.

На данной момент сформировавшимися методами идентификации можно назвать:

идентификация по отпечатку пальца, идентификация по узору руки и по сетчатке глаза, остальные способы можно назвать перспективными, но они требуют необходимой доработки.

СКАНЕРЫ ДЛЯ ПОИСКА УЯЗВИМОСТЕЙ БЕЗОПАСНОСТИ И НЕПРАВИЛЬНОЙ КОНФИГУРАЦИИ

Данцев Никита Сергеевич, курсант 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Хакерская атака – это комплекс действий, направленных на поиск уязвимостей в цифровых системах, например, на компьютерах, смартфонах, планшетных устройствах или даже целых компьютерных сетях. Под хакерской атакой в настоящее время понимается «Покушение на систему безопасности», и склоняется скорее к смыслу следующего термина Крэкерская атака. Это произошло из-за искажения смысла самого слова «хакер».

Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым или элегантным способом; слово hack пришло из лексикона хиппи, в русском языке есть идентичное жаргонное слово «врубаться» или «рубить в …» Начиная с конца XX века в массовой культуре появилось новое значение — «компьютерный взломщик», программист, намеренно обходящий системы компьютерной безопасностиhacker (computersecurity).

Крэкерская атака — действие, целью которого является захват контроля (повышение прав) над удалённой/локальной вычислительной системой, либо её дестабилизация, либо отказ в обслуживании.

Сегодня термин «хакерство» обычно употребляется в контексте противоправных действий, а хакерами называют киберпреступников, которые стремятся получить финансовую выгоду, выразить протест, собрать определенную информацию (то есть занимаются кибершпионажем) или просто хотят развлечься.

Многие склонны думать, что типичный хакер представляет собой талантливого молодого самоучку или одиозного программиста, способного специальным образом модифицировать аппаратное или программное обеспечение, чтобы использовать его в целях, изначально не заложенных производителем.

Хакерские атаки обычно имеют технический характер (как, например, вредоносная реклама, которая внедряет на компьютер опасные объекты в теневом режиме и не требует участия пользователя). Однако хакеры также могут прибегать к психологическим методам, чтобы обманным путем заставить пользователя открыть вредоносное вложение или предоставить конфиденциальные данные. Такие методы называют методами социальной инженерии. Социальная инженерия - это описание методов, которые злоумышленники используют, чтобы заставить жертв нарушить протокол безопасности или отказаться от личной информации. Есть много тактик, которые ведут к этой цели, и они полагаются на психологические манипуляции, такие как соблазнение жертв, играя на их жадности, тщеславии или их готовности помочь кому-то.

«Хакерство» – это общий термин, обозначающий деятельность подавляющего большинства вредоносных объектов, а также кибератаки на компьютеры частных лиц, предприятий и государственных учреждений. Помимо социальной инженерии и распространения вредоносной рекламы, к часто используемым хакерским методам относятся:

- Ботнеты
- Программы-угонщики браузеров
- DDoS-атаки

- Программы-вымогатели
- Руткиты
- Троянские программы
- Вирусы
- Сетевые черви

Ботнеты- это сети компьютеров, зараженных агентом ботнета, которые находятся под скрытым контролем третьей стороны. Они используются для выполнения различных команд, заказанных злоумышленником. Наиболее распространенными видами использования ботнетов являются криминальные операции, требующие распределенных ресурсов, такие как DDoS-атаки на выбранные цели, спам-кампании и мошенничество с кликами. Часто агент ботнета заказывается для загрузки и установки дополнительных полезных нагрузок или для кражи данных с локального компьютера.

С момента заражения агенты ботнета поддерживают контакт со своим удаленным сервером управления и контроля (C&C). Связь может осуществляться различными способами, и киберпреступники продолжают изобретать новые способы сокрытия своих каналов передачи данных. Там было несколько необычных способов с помощью социальных медиа, таких как Twitter или reddit, чтобы отправить команды. Однако наиболее распространенной реализацией C&C является веб-приложение, с которым клиент связывается посредством простых HTTP-запросов.

Угонщик браузера - тип вредоносного ПО, которое овладевает контролем над настройками пользовательского браузера и автоматически перенаправляет на сайты, которые пользователь не намеревался посетить.Большинство угонщиков браузеров устанавливаются на компьютер под видом подключаемых модулей, более известных как расширения для браузеров или тулбары. Зачастую эти модули призваны повысить удобство просмотра интернет-страниц с помощью интерактивных компонентов, например, анимаций. Однако некоторые из них могут привести к тому, что ваш компьютер перестанет реагировать или будет отображать всплывающие сообщения и другое нежелательное содержимое.

Распределенная атака отказа в обслуживании (DDoS) - это сетевая атака, в которой субъекты угроз заставляют многочисленные системы (обычно зараженные вредоносными программами) отправлять запросы на определенный веб-сервер, чтобы разбить, отвлечь или нарушить его достаточно, чтобы пользователи не могли подключиться к нему. DDoS, или распределенные Отказ в обслуживании, который представляет собой вредоносную сетевую атаку, в которой участвуют хакеры, заставляющие многочисленные интернет-соединения подключаться устройства для отправки сетевых запросов связи на один конкретный сервис или веб-сайт с намерением подавляющего это с ложным трафиком или запросами. Это имеет эффект связывания всех доступных ресурсов для решения этих проблем запросов, а также сбой веб-сервера или отвлечение его достаточно, чтобы обычные пользователи не могли создать соединение между свои системы и сервер.

Чтобы осуществить DDoS-атаку, хакерам нужна армия зомби-компьютеров, чтобы выполнить их требования. Хакеры используют то, что мы называем a DDoSToolчтобы поработить компьютеры и построить свою армию. Это зомби-сеть ботов (ботнет) общаться сервер команд и управления (C&C), ожидающий команды от хакера, который запускает ботнет. В случае из DDoS-атаки может случиться, что десятки тысяч или даже миллионы ботов работают одновременно, чтобы отправить большие объемы сетевого трафика в направлении целевого сервера. Обычно, но не всегда, оригинальное заражение DDoSTool не пытается украсть данные или иным образом повредить хост. Вместо этого он лежит в спячке, пока его не призовут участвуйте в DDoS-атаке.

Мотивы, стоящие за атакой на веб-сайт или услугу, различаются. Активисты будут использовать DDoS, чтобы сделать политическое заявление против организации или правительства. Есть преступники, которые делают это, чтобы держать коммерческий сайт в заложниках, пока они получите выкупную выплату. Недобросовестные конкуренты использовали DDoS для грязной игры против конкурирующих компаний. Иногда DDoS-это

еще и стратегия отвлечения внимания администраторов сайта, позволяющая злоумышленнику подбросить другое вредоносное ПО такие как adware, spyware,вымогателей, или даже унаследованный вирус .

Вымогательство вредоносных программ, или вымогателей, является тип вредоносного ПО, которое не позволяет пользователям получить доступ к своей системе или личным файлам и требует оплаты выкупа в приказываю восстановить доступ. Самые ранние варианты вымогателей были разработаны в конце 1980-х годов, и оплата должна была быть отправлено по улиточной почте. Сегодня вымогатели авторы приказывают, чтобы оплата была отправлена с помощью криптовалюты или кредитной карты. Существует несколько различных способов, которыми вымогатели могут заразить ваш компьютер. Одним из самых распространенных методов на сегодняшний день является через вредоносный спам, или malspam, который является нежелательная почта, которая используется для доставки вредоносных программ. Электронная почта может включать в себя заминированные вложения, такие как PDF-файлыили документы Word. Он также может содержать ссылки на вредоносные веб-сайты.

Malspam использует социальную инженерию для того, чтобы обмануть людей в открытии вложений или нажав на ссылки появившись как законный—будь то, казалось бы, от надежного учреждения или друга.Киберпреступники используют социальную инженерию в других типах атак вымогателей, таких как выдача себя за ФБР с целью напугайте пользователей, чтобы заплатить им сумму денег, чтобы разблокировать их файлы.

Еще одним популярным методом заражения, достигшим своего пика в 2016 году, является мальвертизация.Malvertising, или вредоносная реклама, является использование интернет-рекламы, чтобы распространяйте вредоносные программы, не требуя почти никакого взаимодействия с пользователем. Во время просмотра веб-страниц, даже законных сайтов, пользователи могут быть направлены на криминальные серверы, даже не нажимая на рекламу. Сведения каталога этих серверов о компании компьютеры-жертвы и их расположение, а затем выберите вредоносное ПО, которое лучше всего подходит для доставки. Часто, что вредоносные программы это вымогатели.

Malvertising часто использует зараженный iframe, или невидимый элемент веб-страницы, чтобы сделать свою работу. Iframe перенаправляется на целевую страницу эксплойта, и вредоносный код атакует систему с целевой страницы с помощью набора эксплойтов. Все это происходит без ведома пользователя ,поэтому его часто называют загрузкой на диске.

Сканеры для поиска уязвимостей безопасности и неправильной конфигурации Категории: Статьи по информационной безопасности В этой статье приведен список зарубежных сканеров, которые помогут обнаружить уязвимости безопасности и неправильную конфигурацию. Читатели также познакомятся с характерными чертами данных программ. Kubernetes на данный момент стал одной из лучших платформ для оркестрации контейнеров. Более 80% организаций в мире пользуются его услугами. Kubernetes автоматизирует процесс настройки и управления контейнерами. Помимо удобства и простоты использования безопасность также является одним из важных компонентов любого приложения на основе контейнеров. Разработчики должны знать, как обеспечить надежную защиту программам, принадлежащим к группе Kubernetes. За последние несколько лет количество проблем, связанных с безопасностью приложений, росло в геометрической прогрессии. Таким образом, многие компании уделяют огромное внимание вопросам защиты своих продуктов. В чем заключает принцип работы Kubernetes? Он назначает IP-адрес каждому порту в кластерах и обеспечивает их IP-безопасность. Однако Kubernetes способен обеспечить только базовый уровень защиты. К сожалению, платформа не обладает такими функциями, как расширенный мониторинг системы и соблюдение дополнительных политик безопасности. Стоит отметить, что многие сторонние сканеры с открытым исходным кодом могут помочь пользователю защитить его кластеры Kubernetes. Вот несколько преимуществ использования сканеров Kubernetes: обнаруживают

неправильную конфигурацию и уязвимости в кластере, контейнерах и подах; предоставляют решения для изменения неправильной конфигурации и устранения уязвимостей; уведомляют пользователя о состоянии кластера в режиме реального времени; команда DevOps имеет возможность осуществлять разработку и развертывание приложений в кластере Kubernetes, находясь в полной безопасности; помогают избежать сбоя в работе кластера, обнаруживая проблемы на ранней стадии. Настала пора взглянуть на инструменты, которые помогут пользователям найти уязвимости в системе безопасности и неверную конфигурацию приложений. Именно эти программы способны обеспечить защиту приложениям на основе контейнеров.

1. **KubeHunterKubeHunter** – это инструмент поиска уязвимостей AquaSecurity в кластере Kubernetes. Он пригодится для получения дополнительных сведений об уровне безопасности приложения. Этот инструмент предлагает несколько вариантов сканирования, таких как удаленное, чересстрочное, сетевое, на выявление определенных уязвимостей. Он содержит список активных и пассивных тестов, которые помогут выявить большинство уязвимостей, вероятно присутствующих в кластере Kubernetes. Есть несколько способов, с помощью которых пользователь может запустить сканер: Можно скачать архив, распаковать его содержимое и использовать файл формата pip для прямой установки KubeHunter на машину с сетевым доступом к кластеру Kubernetes. После установки человек имеет возможность сразу осуществить сканирование для поиска уязвимостей. Второй способ, как можно запустить KubeHunter, — это использовать контейнер docker. Пользователь устанавливает KubeHunter непосредственно на машину, а затем исследует локальные сети для сканирования кластеров. И третий способ – это запустить KubeHunter в качестве пода внутри своего кластера Kubernetes. Это поможет пользователю найти уязвимости в любых пакетах приложения.
2. **KubeBenchKubeBench** – это сканер с открытым исходным кодом, который проверяет, соответствует ли развертывание приложения стандартам безопасности CIS (CenterforInternetSecurity). Он поддерживает бенчмарк-тесты нескольких версий Kubernetes. Кроме того, сканер также указывает на ошибки в работе приложения и помогает их исправить. Он предоставляет решения для исправления имеющихся проблем. Этот инструмент проверяет правильность авторизации и аутентификации пользователя, а также уровень шифрования данных. Это гарантирует, что развертывание приложения соответствует правилам и стандартам CIS. Особенности KubeBench: был создан на базе языка Go; способен осуществить сканирование подов и мастер-узлов Kubernetes; доступен в качестве контейнера; легко можно изменить параметры сканирования; полученный результат анализа можно просмотреть в формате JSON.
3. **CheckovChekov** – это сканер, который используется для поиска и предотвращения неправильной конфигурации облака во время сборки для Kubernetes, Terraform, Cloudformation и других языков инфраструктуры как кода. Он был написан на языке Python с целью повышения уровня безопасности и изменения параметров приложения для его соответствия всем стандартам подобных программ. Пользователь проводит сканирование с помощью инструмента Chekov для анализа инфраструктуры как кода. Особенности сканера: прост в использовании, имеет открытый исходный код; более 500 встроенных политик безопасности; помогает соблюдать требования AWS, Azure и GoogleCloud; поддерживает несколько форматов вывода полученных данных – CLI, JUnit XML, JSON; можно интегрировать сканирование в CI/CD-пайплайн; проводит сканирование папки, где хранятся файлы Terraform&Cloudformation.
4. **MKIT MKIT**расшифровываетсякак Managed Kubernetes Inspection Tool. Этот инструмент помогает быстро обнаружить ключевые риски безопасности кластеров Kubernetes и их ресурсов. Он предлагает пользователю простые способы оценки неправильной конфигурации в кластере и рабочих нагрузках. Инструмент имеет специальный веб-интерфейс, который доступен по адресу «http://localhost:8000» (по умолчанию). В нем человек сможет получить представление о неудачных и уже

осуществленных проверках. Более того, пользователь также может узнать об уязвимых и неуязвимых ресурсах. Особенности MKIT: был создан на основе библиотек и инструментов с открытым исходным кодом; легко устанавливается и прост в использовании; совместим с несколькими поставщиками Kubernetes – AKS, EKS и GKE; хранит конфиденциальные данные внутри контейнера; есть веб-интерфейс.

5. **KubeiKubei** используется для оценки непосредственных рисков в кластере Kubernetes. Большая часть инструмента написана на языке программирования Go. Он охватывает все бенчмарки CIS Docker. Инструмент сканирует все изображения, используемые кластером Kubernetes, а также подами приложений и системы. Пользователь имеет возможность провести несколько типов сканирования в зависимости от: уровня уязвимости, скорости или объема сканирования. В графическом интерфейсе пользователь может просмотреть все уязвимости, которые имеются в кластере, а также способы их устранения. Особенности Kubei: сканер с открытым исходным кодом; проводит сканирование общедоступных изображений, размещенных в реестре пользователя; контролирует состояние кластера в режиме реального времени; есть веб-интерфейс для визуализации результатов сканирования; предоставляет несколько пользовательских опций для проведения различных типов анализа безопасности приложения.

6**.** **KubeScanKubeScan** – это сканер контейнеров, который доступен пользователю сам в виде контейнера. Человек устанавливает его в новый кластер, после чего он может сканировать рабочие нагрузки, которые в данный момент выполняются там. Сканер оценивает уровень безопасности и предоставляет результаты сканирования в удобном веб-интерфейсе. Оценка риска варьируются от 0 до 10, где 0 означает отсутствие риска, а 10 – высокую его степень. Формула для выставления общей оценки, которая применяется в KubeScan, была позаимствована у CCSS (CommonConfigurationScoringSystem) Kubernetes. Она похожа на CVSS (CommonVulnerabilityScoringSystem). Учитываются более 30 различных параметров безопасности, таких как политики Kubernetes и уровни привилегий. Кроме этого, сканер создает базовый уровень риска для получения общей картины уровня защиты приложения. Особенности KubeScan: инструмент с открытым исходным кодом; есть веб-интерфейс, где пользователь может просмотреть информацию об оценке рисков; доступен в виде контейнера в кластере; можно проводить повторное сканирование кластера каждые 24 часа.

7. **KubeauditKubeaudit**, как следует и из его названия, является инструментом аудита кластера Kubernetes с открытым исходным кодом. Он способен обнаружить неправильные настройки безопасности в ресурсах Kubernetes и сообщить пользователю о том, как их устранить. Программа была написана на языке Go, поэтому можно использовать ее в качестве пакета Go или инструмента командной строки. Пользователь также может установить его на свой компьютер. Инструмент предлагает различные способы сканирования: с запуском приложения от имени пользователя, с предоставлением доступа только для чтения к корневой файловой системе, без предоставления дополнительных привилегий приложениям в кластере. Все виды сканирования помогают предотвратить общие проблемы безопасности. Kubeaudit имеет обширный список аудиторов, используемых для поиска проблем безопасности кластера Kubernetes, таких как поды SecurityContext. Особенности сканера: инструмент с открытым исходным кодом; есть три режима сканирования – «манифест», локальный, кластерный; способен выявить ошибки в работе приложения, предотвратить их, дать советы по повышению уровня безопасности; есть несколько встроенных аудиторов для проведения аудита контейнеров, подов, пространств имен. 8. KubesecKubesec – это сканер рисков безопасности с открытым исходным кодом для ресурсов Kubernetes. Он проверяет конфигурацию и файлы манифеста, используемые для развертывания приложения и осуществления операций кластера Kubernetes. Пользователь может установить его на свой ПК, используя образ контейнера, двоичный пакет, контроллер доступа в Kubernetes или плагин kubectl. Особенности сканера: инструмент с открытым исходным кодом; идет в комплекте с HTTP-сервером, который по

умолчанию работает в фоновом режиме на порту 8080; может сканировать несколько документов YAML одновременно и предоставить результаты сканирования в одном файле.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Дегтярев Константин Игоревич

Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,

город Москва

1) Киберпреступников не интересуют компьютеры частных лиц

К счастью, этому высказыванию мало кто верит. В данном случае утверждение также ложно.

Разумеется, корпоративные сети интересуют киберпреступников, но их сложнее заразить. Сегодня частные компьютеры так же хорошо подходят в качестве составляющих ботсетей. К тому же очень часто на них хранится много интересных персональных данных, таких как данные доступа к онлайн-магазинам, социальным сетям и учетным записям электронной почты или данные о кредитных картах, из которых киберпреступники могут извлечь выгоду. Поэтому не стоит недооценивать значение частных компьютеров для злоумышленников.

2) Большинство вредоносных программ распространяется по электронной почте

Данный тезис устарел, но, несмотря на это, данной точки зрения придерживается 54% участников опроса. В конце прошлого тысячелетия рассылка вирусов Melissa и I love you по электронной почте стала наиболее популярным способом распространения вредоносных программ. Приблизительно шесть лет назад на смену отправке электронных сообщении с зараженными вложениями пришли сообщения со ссылками на файлы, размещенные на Web-сайтах. Данная тактика позволяла злоумышленникам обходить очень эффективные спам-фильтры и доставлять сообщения ничего не подозревающему пользователю. С другой стороны, многие пользователи стали очень осторожны с сообщениями от неизвестных отправителей и в лучшем случае сразу удаляют их, не открывая. В большинстве случаев ссылки в электронных сообщениях направляют на вредоносные Web-сайты. Таким образом, появляются дополнительные возможности для поиска жертв: например, социальные сети, оптимизация поисковых запросов, ошибочные домены и т.д. Вредоносные программы находятся на Web-сайтах, а Web-сайты являются вектором заражения номер один.

3) Заражение ПК не происходит при загрузке зараженного Web-сайта

То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов "попутной загрузки" возможно уже на протяжении многих лет. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке".Во-первых, Web-сайты, созданные специально с целью заражения ПК.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое заражение ПК вредоносной программой. Преимуществом данного способа для киберпреступников является то, что им не приходится рекламировать Web-сайт. Для дальнейшей манипуляции данным Web-сайтом злоумышленникам необходимо в него внедриться. Если Web-сайт хорошо защищен, то осуществить такое внедрение очень сложно.

4)Большинство вирусов и вредоносных программ распространяются посредством зараженных файлов на файлообменниках

Бесспорно, определенное количество вредоносных программ распространяется через такие системы обмена файлами, как торренты и одноранговые сети. Неудивительно, что 48% участников опроса считают, что данный способ является основным в распространении вредоносного ПО. Наверняка тот или другой пользователь уже хотя бы раз заражал свои компьютер вирусом после посещения подобных сайтов. Однако данный тезис также ложен и является мифом, поскольку большинство вредоносных программ распространяется через вредоносные Web-сайты.

5) Мой брандмауэр защищает меня от заражения при "попутной загрузке"

Данному утверждению верит 26% опрашиваемых. Этот тезис ложен. Брандмауэры – это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной Web-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных задании вредоносной программой и, например, отправку данных злоумышленникам, если речь идет о шпионских программах.

6) Если не открывать зараженные файлы, то ПК нельзя заразить

Это высказывание основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно лишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открытия зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

7) Большинство вредоносных программ распространяется через USB-накопители

В последние годы популярность флешек и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. Поэтому настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя.

8) Я не посещаю странные Web-сайты, поэтому мне не угрожает заражение при "попутной загрузке"

Данное утверждение можно опровергнуть так же, как и шестой тезис. Тематика Web-сайта не играет для киберпреступников никакой роли. Они заинтересованы в том, чтобы с минимальными затратами заразить вредоносными кодами максимальное количество посетителей. Это удается злоумышленникам, помимо всего прочего, с помощью манипуляции с баннерами и постоянных атак крупных доменов. В случае успеха и получения доступа они внедряют вредоносный код с помощью так называемых эксплойт-инструментов, и специальные знания для этого не требуются. Web-саиты, которые на протяжении многих лет считались достойными доверия, могут быть взломанными и в результате таить в себе опасность заражения.

9) Обеспечение информационной безопасности в облачной инфраструктуре

При защите данных в публичном облаке, я выделяю два направления, так называемую безопасность облака, и безопасность в облаке. Безопасность в облаке обеспечивает провайдер, и мы на нее влиять никак не можем, поэтому здесь важно грамотно подойти к выбору поставщика облачных услуг и установлению с ним отношений. Для безопасности

облака, в той части, где мы можем обеспечивать дополнительную безопасность, с помощью специальных программных средств и политик, сформулированы также свои рекомендации. Рассмотрены подходы к выбору облачного провайдера. Разработан ряд критериев по ИБ, которым должны соответствовать облачные провайдеры и на которые можно опираться при выборе поставщика облачных услуг.

Особое внимание уделено установлению партнерских отношений с провайдером, т.к. доверие к провайдеру и партнерские отношения исключительно важны, в том числе и для обеспечения ИБ данных. Доверие провайдеру очень важный пункт, но лучше чтобы дружба была подкреплена грамотно заключенным договором о предоставлении услуг и соглашением об уровне обслуживания (SLA). Данные документы могут иметь решающее значение при возникновении спорных ситуаций, в том числе связанных с ответственностью в вопросах ИБ.

10) Целостность информации

Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

ОБЛАЧНЫЕ СЕРВИСЫ И ФАНТАСТИЧЕСКИЕ ВОЗМОЖНОСТИ ИНТЕРНЕТА

Демиденко Данил Дмитриевич, студент второго курса
Научный руководитель Ковалева Лариса Дмитриевна, преподаватель
Научный руководитель Семенов Андрей Владимирович, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Облачные технологии – это одна из самых быстро развиваемых современных технологий в сфере IT. Крупнейшие компании — Google, Apple, Microsoft, Amazon — бросают целые армии разработчиков в бой на этом поле рынка. Интерес пользователей к облачным технологиям постоянно растет.

В облачных вычислениях обычно выделяют три отдельные категории или уровня:

1. Низший уровень. Иногда называется «Инфраструктура как услуга». На этом уровнепользователи получают базовые вычислительные ресурсы – например, процессоры и устройства для хранения информации – и используют их для создания своих собственных операционных систем и приложений. Каждый, кому требуется интернет-сервер, может получить его практически сразу. Для этого достаточно заказать соответствующую услугу через Интернет, причем оплачивать лишь фактически используемые вычислительные мощности. Все затраты, связанные с закупкой, установкой, наладкой и поддержанием работы оборудования, отпадают. Пакет облачных сервисов представлен на рисунке 1.

Рисунок 1 - Пакет облачных сервисов

2. Средний уровень. Платформа как услуга. На этом уровне пользователи имеют возможность устанавливать собственные приложения на платформе, предоставляемой провайдером услуги. Распространение сервиса PaaS (платформа как услуга) революционизирует проектирование и разработку программных приложений, которые

доступны через Интернет. PaaS решает проблему масштабирования приложений, предоставляет разработчикам богатые библиотеки готовых решений, существенно упрощает отладку систем и их ввод в эксплуатацию и т.п. То, для чего раньше требовались месяцы, теперь решается за недели, а порой и дни. Стоимость разработок сокращается в разы. Освобождаясь от решения рутинных технических задач, разработчики получают возможность сосредоточиться на самих задачах, что переводит веб-технологии на более высокий качественный уровень.

3. Высший уровень. «Программное обеспечение как услуга». В облаке хранятся не только данные, но и связанные с ними приложения, а пользователю для работы требуется только веб-браузер. Лучшими примерами такого подхода являются GoogleAppsforEducationиMicrosoftLive@edu, предоставляющие как средства поддержки коммуникации, так и офисные приложения. Приложения для решения повседневных задач, доступные прежде лишь крупным бизнес-структурам и банкам, становятся доступны массовому потребителю.по разумной цене крайне необходимую им цифровую инфраструктуру промышленного уровня.

В настоящее время особо остро ощущается то, как «жизнь уходит» в онлайн. Пандемия и невозможность проводить время с близкими толкают людей к тому, что в онлайне сейчас организуют вечеринки и даже свадьбы. Увеличивается спрос на онлайн-развлечения, популярность приобретают сервисы для онлайн-трансляций и приложения для видеоконференций, которые теперь часто используются не только для работы. Самый популярный сервис для стримингаTwitch в апреле 2020 года побил рекорд по одновременному онлайну пользователей, достигнув планки в 4 млн. Люди начинают стримить кулинарные вебинары, посиделки с друзьями, появляются обучающие и образовательные стримы. Все это по праву становится частью индустрии. И мы убеждены, что подобный тренд будет только нарастать.

Иногда пользователи начинают делать в онлайне и совсем необычные для него вещи: проводить виртуальные вечеринки в компьютерном симуляторе Sims, справлять свадьбы вмногопользовательских онлайн-играх, например в FinalFantasy, и даже угадывать пол своего будущего ребенка, транслируя это на Twitch. Некоторые проводят уроки по геометрии для своих учеников в VR-игре Half-Life: Alyx.

В настоящее время, в связи со сложившейся ситуацией, для поддержания образовательных и иных процессов используются платформы, работающие на облаке, в том числе и MS Teams. Сервис представлен в ноябре 2016 года, он объединяет в рабочем пространстве чат, встречи, заметки и вложения. Провести тест, работать с цифровой доской, поделиться информацией со своего экрана можно, не выходя из приложения. Видеоконференции доступны и в других приложениях, но в MicrosoftTeams их легко запланировать через календарь, настроить уведомление внутри платформы или по почте, а чтобы быстро подключить ученика к уроку или родителя к собранию, нужно упомянуть его имя через @. MicrosoftTeams является частью пакета Office 365, поэтому в отличие от бесплатной версии Zoom бесплатный план Office уже включает доступ к облачному хранилищу объемом 1 ТБ. Все проекты и документы будут автоматически сохраняться в облаке. Всё это позволяет Teams быть удобной, функциональной и главное конкурентной платформой.

Преимущества использования облачных услуг.

- Резервирование и сохранение целостности размещенных пользователем данных производятся исключительно провайдером данного центра.
- Пользователь оплачивает только то место в «облаке», которое он фактически занимает своими файлами, а не за аренду самого сервера. Сохраняет свободное место на жестких дисках.
- При поездках не нужно возить с собой флэш-накопители.
- Круглосуточный доступ к своим файлам, данные доступны из любого места с использованием целого диапазона различных устройств.

- Данные не ограничены жестким диском на компьютере одного пользователя.
- Снижаются затраты на приобретение дорогостоящего оборудования.
- Не нужно беспокоиться о создании резервной копии данных или о возможности их потери

Недостатки облачного хранения данных

- Необходимо стабильное интернет-соединение;
- Как правило, бесплатно предоставляется только до 5-7 Гб свободного места навиртуальном сервере;
- Привыкание к пользовательскому веб-интерфейсу компании, которая предоставляетуслуги по хранению информации в облаке.

Список использованных источников

1. Дунаев В. В. Сценарии для Web-сайта PHP и JavaScript. – 2-е изд. перераб. и доп. – СПБ.: БХВ-Петербург, 2017. – 576 с.: ил.

2. Колисниченко Д.А., PHP и MySQL. Разработка веб-приложений / Д.А. Колесниченко. - М., 2017. – 592 с.

3. Википедия – свободная энциклопедия: [Электронный ресурс]. - https://ru.wikipedia.org/

4. Могилев А. В., Листрова Л. В. Технологии поиска и хранения информации. Технологии автоматизации управления; БХВ-Петербург - Москва, 2019. - 320 с.

5. 9. Риз Джордж Облачные вычисления; БХВ-Петербург - Москва, 2018. - 288 с.

ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Джаримов Аслан Инверович, курсант 903 учебного взвода МосУ МВД имени В.Я.Кикотя

Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Программная защита информации — это система специальных программ, реализующих функции защиты информации. Выделяют следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

1)защита информации от несанкционированного доступа;

2)защита информации от копирования;

3)защита информации от вирусов;

4)программная защита каналов связи.

5)Защита информации от несанкционированного доступа

Программные средства включают программы для идентификации пользователей, контроля доступа, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и другие. Преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию.

Недостатки – использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств).

Центральным для программно-технического уровня является понятие сервиса безопасности, к которому относятся следующие основные и вспомогательные сервисы: идентификация и аутентификация, протоколирование и аудит, шифрование, контроль целостности, экранирование, обеспечение отказоустойчивости, туннелирование и управление, RFID – технологии, штрих – технологии.

Совокупность перечисленных выше сервисов безопасности называют полным набором. Считается, что его, в принципе, достаточно для построения надежной защиты на программно-техническом уровне, правда, при соблюдении целого ряда дополнительных условий (отсутствие уязвимых мест, безопасное администрирование и так далее)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Донцов Денис Олегович, студент 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Информационная безопасность занимается защитой информации от несанкционированного доступа. Это часть управления информационными рисками и включает в себя предотвращение или снижение вероятности несанкционированного доступа, использования, раскрытия, нарушения, удаления, повреждения, модификации, проверки или записи.

Если инцидент безопасности действительно происходит, специалисты по информационной безопасности участвуют в снижении негативного воздействия инцидента. Примечание информация может быть электронной или физической, материальной или нематериальной.

В то время как основной целью любой программы информационной безопасности является защита конфиденциальности, целостности и доступности информации (триада ЦРУ), поддержание организационной производительности часто является важным фактором. Это привело к тому, что индустрия информационной безопасности предложила руководство, политику информационной безопасности и отраслевые стандарты по паролям, антивирусному программному обеспечению, брандмауэрам, шифровальному программному обеспечению, юридической ответственности и осведомленности о безопасности для обмена передовым опытом.

Информационная безопасность достигается за счет структурированного процесса управления рисками, который:

1) Идентифицирует информацию, связанные с ней активы, а также угрозы, уязвимости и последствия несанкционированного доступа

2) Оценивает риски

3) Принимает решения о том, как устранять или лечить риски, то есть избегать, смягчать, делиться или принимать

4) При смягчении выбирает, проектирует и реализует средства контроля безопасности

5) Контролирует деятельность и вносит коррективы для решения любых новых проблем, изменений или улучшений

Кто управляет информационной безопасностью?

Угрозы информационной безопасности проявляются во многих формах, не ограничиваясь стихийными бедствиями, неисправностями компьютеров или серверов и физическими кражами. В то время как бумажные компании все еще существуют, постоянно растущая зависимость от информационных систем привела к тому, что информационная безопасность стала ключевым фактором в управлении рисками кибербезопасности и вызвала потребность в специализированных специалистах по ИТ-безопасности.

Эти специалисты по безопасности информационных технологий занимаются вопросами безопасности данных, безопасности приложений, сетевой безопасности, компьютерной безопасности и физической безопасности. Поймите, что данные, приложения и компьютеры распространяются далеко за пределы того, что традиционно считается компьютером. Смартфоны, столы и другие мобильные устройства являются такой же частью компьютера, как сервер или мэйнфрейм, и подвержены вредоносным кибератакам, которые могут получить доступ к конфиденциальной информации, критической информации,

информационным активам или контролю над важными внутренними компьютерными системами.

Это, в сочетании с растущим количеством утечек данных, привело к увеличению спроса на сложное планирование защиты данных и растущему спросу специалистов по кибербезопасности на понимание информационной безопасности. Растет число сертификатов информационной безопасности, и работодатели часто предпочитают сотрудников с сертификацией, подтверждающей знание лучших практик. Существуют широкие сертификаты, такие как CertifiedInformationSystemsSecurityProfessional (CISSP), и конкретные, которые охватывают обеспечение информационной безопасности, сетевую безопасность, тестирование безопасности, бизнес-аудит, планирование непрерывности бизнеса, тестирование безопасности, планирование реагирования на инциденты, кражу личных данных, оценку рисков, системы обнаружения вторжений, нарушения безопасности и все другие меры безопасности. Общие роли, требующие специальных знаний в области управления информацией, включают главного сотрудника по информационной безопасности (CSO), главного сотрудника по информационной безопасности (CISO), инженера по безопасности, аналитика информационной безопасности, администратора систем безопасности и консультанта по ИТ-безопасности.

Что такое угрозы информационной безопасности?

Угрозы могут проявляться во многих формах, включая атаки на программное обеспечение, кражу личных данных, саботаж, физическое воровство и вымогательство информации:

Программные атаки на информационную безопасность включают вирусы, вредоносные программы, черви, программы-вымогатели, такие как WannaCry или троянский конь.

Фишинговые электронные письма или веб-сайты часто направлены на кражу интеллектуальной собственности или ввод учетных данных для получения несанкционированного доступа. Социальная инженерия является одной из крупнейших киберугроз и от нее трудно защититься традиционными мерами безопасности

Саботаж, как и атаки типа отказа в обслуживании, часто направлен на снижение доступности ключевых информационных активов, снижение доверия или производительности организации до тех пор, пока не будет получен платеж в обмен на возврат услуг организации

Кража информации и оборудования становится все более распространенным явлением, поскольку большинство устройств в настоящее время являются мобильными по своей природе, как смартфоны или ноутбуки

Вымогательство информации включает в себя получение доступа к конфиденциальной информации, а затем удержание ее в качестве выкупа до тех пор, пока не будет произведена оплата

Существует много способов защиты от кибератак, но главная угроза для любой организации-это ее пользователи или внутренние сотрудники, которые подвержены социальной инженерии или фишингу. Вот почему обучение по вопросам кибербезопасности и контроль безопасности важны на всех уровнях вашей организации.

Как вы реагируете на угрозы информационной безопасности?

Когда угроза идентифицирована у вас есть выбор:

1) Снижение или смягчение риска путем внедрения гарантий или контрмер устранение или уменьшение угроз и уязвимостей

2) Переуступка или передача риска другому субъекту или организации путем приобретения страхования или аутсорсинга

3) Примите риск, когда стоимость контрмеры больше, чем возможная стоимость потерь из-за уязвимости или кибератаки

С введением Общего регламента защиты данных (GDPR) Европейским парламентом и Советом в 2016 году необходимость реагирования на нарушения информационной

безопасности стала нормативным требованием для любого бизнеса, работающего в ЕС. Теперь компании обязаны:

1) предоставлять уведомления о нарушении данных

2) назначать сотрудника по защите данных

3) требовать согласия пользователя на обработку данных

4) анонимизировать данные для обеспечения конфиденциальности

Это делает комплексный план обработки инцидентов и комплексное обнаружение утечек данных обязательным требованием для большинства глобальных компаний.

Как вы определяете информационную безопасность?

Существует много способов определения информационной безопасности, но как Национальный институт стандартов и технологий (NIST), так и Национальный глоссарий по обеспечению информационной безопасности (IA) определяют информационную безопасность как "защиту информации и информационных систем от несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения с целью обеспечения конфиденциальности, целостности и доступности."

Каковы основные принципы информационной безопасности?

Конфиденциальность, целостность и доступность, также известные как триада ЦРУ, лежат в основе информационной безопасности. Тем не менее, существует дискуссия о том, достаточно ли триада ЦРУ учитывает быстро меняющиеся технологические и бизнес-требования, а также взаимосвязь между безопасностью и конфиденциальностью. Были предложены и другие принципы, такие как подотчетность, и отказ от ответственности не очень хорошо вписывается в эти три основные концепции.

Что такое конфиденциальность?

Конфиденциальность заключается в том, чтобы не предоставлять информацию или раскрывать ее неуполномоченным лицам, организациям или процессам. Хотя эти слова похожи на конфиденциальность, они не должны использоваться взаимозаменяемо.

Конфиденциальность - это компонент конфиденциальности, который реализует меры безопасности для защиты от несанкционированного просмотра. Конфиденциальность пользователей становится все более важной частью конфиденциальности из-за GDPR и других нормативных требований.

Другие примеры конфиденциальности включают защиту от кражи ноутбука, кражи пароля и других методов управления безопасностью.

Что такое целостность?

Целостность или целостность данных связана с поддержанием, обеспечением, точностью и полнотой данных на протяжении всего их жизненного цикла. Это означает внедрение средств контроля безопасности, которые гарантируют, что данные не могут быть изменены или удалены неавторизованным лицом или незамеченным способом.

Что такое доступность?

Чтобы любая информационная система была полезной, она должна быть доступна, когда это необходимо. Это означает, что компьютерные системы, которые хранят и обрабатывают информацию, средства контроля безопасности, которые ее защищают, и каналы связи, которые к ней обращаются, должны функционировать по требованию.

Компании и их клиенты все больше полагаются на системы высокой доступности в режиме реального времени 24/7. Это означает, что специалисты по информационной безопасности все больше озабочены обеспечением доступности путем предотвращения перебоев в подаче электроэнергии, сбоев оборудования и атак типа "отказ в обслуживании". Доступность часто рассматривается как наиболее важная часть успешной программы информационной безопасности, поскольку в конечном счете именно конечные пользователи должны иметь возможность использовать эту информацию.

Что такое неотречение?

Неотречение- это заимствованный из права термин, подразумевающий намерение человека выполнить свои обязательства по договору и то, что одна из сторон не может отрицать получение или отправку сделки.

Как информационная безопасность сочетается с управлением информационными рисками?

Управление информационными рисками-это процесс выявления уязвимостей и угроз информационным ресурсам, используемым организацией, и принятия каких-либо контрмер для снижения риска до приемлемого уровня на основе ценности информации для организации.

В любом процессе управления рисками есть два основных соображения:

Процесс управления рисками носит непрерывный и итеративный характер, он должен повторяться бесконечно по мере появления новых угроз и уязвимостей

Выбор используемых контрмер или средств контроля должен обеспечивать баланс между производительностью, затратами, эффективностью и информационной ценностью защищаемого актива

Анализ и оценка рисков имеют врожденные ограничения, поскольку при возникновении инцидентов безопасности они возникают в контексте и могут исходить от непредсказуемых или неожиданных угроз, таких как плохо настроенные ведра S3 или внешние злоумышленники.

Вероятность того, что угроза использует уязвимость для причинения вреда, создает риск. В контексте информационной безопасности воздействие заключается в потере конфиденциальности, целостности или доступности или во всех других возможных потерях (например, репутационный и финансовый ущерб). Примечание: Невозможно ни идентифицировать, ни смягчить все риски. Этот оставшийся риск называется остаточным риском.

Список использованных источников

1. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. − М.: ДМК Пресс, 2008. – 544 с.

2. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М.: Книжный мир, 2009. – 352 с.

ТАЙМ-МЕНЕДЖМЕНТ: ИСТОРИЧЕСКИЕ АСПЕКТЫ И СОВРЕМЕННЫЙ ПОДХОД

Дубинина Анна, студентка 3-го курса
Научный руководитель Черненко Виктория Александровна
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

История развития тайм-менеджмента берет начало в Древнем мире. Уже в самом начале нашей эры (т.е. около 2000 лет назад) римский мыслитель Сенека предложил в письме поэту Люцелию следующие идеи:

Разделять все время на потраченное хорошо, плохо и бесполезно;

Вести постоянный учет времени в письменном виде;

Прожив определенный период, оценивать его с точки зрения заполненности.

Итальянский ученый и писатель Альберти, живший в XV веке, утверждал, что люди, умеющие управлять временем с пользой, будут успешны всегда и в любом деле. Для этого, согласно его письмам, необходимо придерживаться двух правил.

Первое — каждый день с утра составлять список дел.

Второе — упорядочивать дела в порядке уменьшения важности. Такие действия, как сон, еда и развлечения писатель считал менее важными, чем работа. Сам он строго придерживался своих принципов.

Заметно повлияло на историю развития тайм-менеджмента появление промышленности. Необходимость управлять слаженной работой сотен людей заставила искать новые способы управления временем. На производствах был введен строгий график, появились расписания, смены.

Бенджамин Франклин, известный политический деятель и ученый, в молодости столкнулся с проблемой нехватки времени. Выход он нашел в ведении собственного дневника, в котором ежедневно отмечал выполнение каждой из 13 добродетелей, которые стремился развивать. Неделя расписывалась на одном расчерченном листке, где каждый столбец соответствовал одному дню.

В 1842 году издан "Трактат о домашнем хозяйстве" Кэтрин Бичер, в нем содержится множество советов о том, какие виды домашних работ выполняет женщина, как эти работы правильно организовать, и с помощью каких приемов можно всё это быстро выполнить.

Например, одним из таких "ускоряющих" ведение домашнего хозяйства рекомендаций являлась т.н. "Кухня Бичер" - кухня, спроектированная с максимальной рациональностью, это система многочисленных и определенным образом организованных полочек, шкафчиков и ящичков

Такая планировка действительно значительно ускоряла все кухонные операции! Она считала, что женщины должны исполнять благородную миссию - исправлять "деградировавших" мужчин, но не через борьбу с ними, а через "сотворение красоты и благополучия", через заботу об этом мире.

«Кухня Бичер» - предшественник современных кухонных гарнитуров, которые спроектированы с максимально эффективной организацией рабочего пространства.

Немалое влияние на тайм-менеджмент оказало открытие Вильфредо Парето знаменитого принципа «20:80». Применяя этот принцип к тайм-менеджменту, Парето пришел к выводу, что 20% всех усилий дают 80% результата, а прочие 80% сил расходуются для получения оставшихся 20% достижений. Отсюда следует вывод о разделении дел по степени важности предполагаемого результата. Подобные идеи лежат в основе многих современных тренингов по управлению временем.

В 1950-е годы генерал и 34-ый президент США (1953-1960) Дуайт Дэвид Эйзенхауэр предложил замечательный инструмент приоритезации повседневных задач и дел, ныне известный как "матрица Эйзенхауэра".

Эйзенхауэру принадлежит высказывание: "Важные дела редко бывают срочными, а срочные редко бывают важными".

Срочные и важные дела – выполняет сам руководитель,

Не срочные и важные – необязательно выполнять сразу, но обязательно самому,

Срочные не важные – их нужно делегировать,

Не срочные и не важные – от их выполнения можно воздержаться.

Термин «тайм-менеджмент» возник в 70-х годах XX-го века, благодаря датскому предпринимателю Клаусу Миллеру. В **1975** г. он изобрел блокнот Time Manager, который являлся прототипом органайзера.

В это же время стали появляться тренинги, обучающие программы. Первыми клиентами Миллера были сотрудники крупнейших авиакомпаний Lufthansa, British Airways.

1989 год - именно в этом году Тим Бернерс-Ли изобрёл Всемирную паутину (WWW), что означало революцию в скорости обмена информацией между людьми. Сейчас интернет наоборот забирает много времени (палка о2х концах, информации много, а качественной мало)

История тайм-менеджмента в СССР началась во времена НЭПа (21-29). Наработки в этой области назывались НОТ, что расшифровывалось как Научная Организация Времени. Следующая волна популярности тайм-менеджмента в СССР пришла вместе с другими новшествами уже во второй половине 80-х.

Школы ТМ

Джулия Моргенстерн. Управлять временем “изнутри наружу” – значит строить такое расписание дня, такой график жизни, которые подходят именно вам. Это значит определить, что важно именно вам, и найти для этой деятельности место в вашей жизни и в вашем расписании, которое будет основываться на ваших уникальных личных потребностях и жизненных целях. И еще это значит – чувствовать себя глубоко удовлетворенным в конце каждого прожитого дня. Давайте сравним беспорядок в шкафу с беспорядком в графике работы.

Другими словами, точно так же, как шкаф является ограниченным пространством, в котором вы должны разместить определенное количество предметов, график или расписание – это ограниченное пространство, в котором вы должны разместить определенное количество задач. Ваша жизнь вовсе не бесконечна. Когда вы думаете о времени подобным образом, оно уже не кажется таким неощутимым и эфемерным. На самом деле, каждый день – просто сосуд, контейнер, блок памяти, обладающий определенной вместимостью, которую вы можете использовать.

Стивен Кови. Рассматривал принципы и ценности как отдельные величины — принципы как внешние и естественные законы, а ценности как внутренние и субъективные, присущие отдельному человеку. Он утверждал, что ценности управляют поведением человека, но принципы, в конечном счете, определяют результат.

Брайан Трейси. «Энергия времени». Метод учит разделять дела на существенные и второстепенные, браться именно за то, что имеет принципиальное значение. Важен первый шаг: нужно научиться пересиливать себя. Законы тайм-менеджмента гласят, что собственное время нужно правильно дозировать и не стоит распылять его на второстепенные задачи. Контроль расхода собственного времени позволит избавиться с хаосом, который создает неразбериха. Все должно делаться в отведенное время. Сложно сконцентрироваться сразу на многих делах и от такой деятельности будет мало толку.

Дэвид Аллен. Подход к управлению временем осуществляется "снизу-вверх" (человек управляет делами и задачами "здесь и теперь", по мере их поступления), - это в первую очередь алгоритм сортировки "входящих" дел, задач, событий и информации.

Основное назначение учения - упорядочить хаос событий таким образом, чтобы максимально концентрироваться на наиболее важных задачах, и эффективно выполнять их. Сам алгоритм состоит из 5 этапов: 1) Сбор; 2) Обработка; 3) Организация; 4) Обзор; 5) Действия.

Основные положения

Самоменеджмент - это последовательное и целенаправленное использование эффективных методов работы в повседневной практике, с оптимальным использованием своих ресурсов для достижения своих же целей.

Основные функции самоменеджмента:

1. Постановка цели – желаемый долгосрочный результат
2. Определение задач– устанавливается краткосрочная цель, которая впоследствии приведет к достижению долгосрочной цели;
3. Планирование – рациональное использование времени (чем лучше спланировано время, тем лучше оно используется);

Основные правила планирования времени:

3.1.Соотношение 60/40-рабочее время планируется на 60%,

3.2.Регулярность – системность - последовательность (доводить до конца начатое дело),

3.3.Реалистическое планирование – ставить реально выполнимые задачи.

3.4.Заполнение потерь времени

3.5.Фиксация результатов вместо действий – в планах необходимо фиксировать результат или цель.

3.6.Срок выполнения – нужно устанавливать точные сроки выполнения для всех видов деятельности,

3.7.Согласованность различных планов во времени

4. Делегирование – передача заданий подчиненным,
5. Реализация и организация - рабочего дня должна отвечать правилам, которые поделены на 3 группы: правила начала дня, правила основной части, правила завершения работы.
6. Контроль необходим для оптимизации трудового процесса.
7. Информация и коммуникация – необходимо разработать рациональный подход к получению, обработке и использованию информации.

Итак, как же Тайм-менеджмент влияет на жизнь? Он помогает людям достигать целей и управлять своей жизнью. При соблюдении правил планирования, человек повышает свою продуктивность, учится грамотно распределять задачи во времени.

Список использованных источников:

1. Брайан Трейси. Мастер времени, 2017. – 144с.
2. https://headlife.ru/taym-menedzhment/
3. Джулия Моргенстерн. Тайм-менеджмент. Искусство планирования и управления своим временем и своей жизнью, 2009. – 230с.
4. http://timestep.ru/2010/11/30/sistema-upravleniya-vremenem-bendzhamina-franklina

ЗАЩИЩЕННОСТЬ И НАДЕЖНОСТЬ СОВРЕМЕННЫХ ОС

Дыков Артем Евгеньевич, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

До того, как начать рассматривать всевозможные уязвимости операционной системы и организационные нюансы надежной системы информационной безопасности, следует обратить внимание на опасности защищенности операционной системы. Степень угрозы непосредственно зависит от того, как работает и используется целевая операционная система, а также какая информация в ней хранится и обрабатывается. Существуют случаи, когда атакуется система, непосредственно работающая в сфере электронного документооборота. Наиболее опасными являются угрозы, когда удаленно может быть получен доступ к правам суперпользователя и изменения данных. . Существуют случаи, когда ОС является платформой интернет-провайдера, при которых атаки на сетевые устройства и программное обеспечение могут быть критичными.

Существуют 3 группы возможностей получения несанкционированного доступа к операционной системе:

- Атаки уровня управления баз данных;
- Атаки на сетевые устройства и программное обеспечение;
- Атаки, эксплуатирующие уязвимости уровня операционной системы;

Типичные атаки на операционную систему

1. Кража ключевой информации

Существует множество методов несанкционированного доступа к информации. Простейшая атака заключается в обыкновенном просмотре злоумышленником пароля. Также есть программа для входа в операционную систему удаленного сервера. Это позволяет вам вводить пароль из командной строки. Такие команды включают, например, команду nwlogin в операционных системах UNIX, предназначенную для входа на серверы NovellNetWare. При использовании с ключом -p вы можете ввести пароль в командной строке. Например, пользователь сервера nwlogin -ppassword. Здесь уже непосредственную играет роль человеческий фактор.

2. Подбор пароля

- Подбор пароля по частоте появления символов и биграмм.
- Прямой выбор паролей и их комбинаций с использованием наиболее часто используемого словаря паролей.
- Выбор пароля с использованием личных данных, таких как дата рождения, место рождения, девичья фамилия матери, любимый фрукт и многое другое.
- Только один пароль тестируется из каждого класса, и выбор пароля с использованием информации о существовании эквивалентных паролей. Это может значительно сократить время итерации.
- Полное перечисление всех возможных вариантов пароля с использованием различных комбинаций, с учетом предыдущего метода выбора. Это самый необоснованный способ из перечисленного.

Очевидно, что значительная часть проблемы заключается в том, что операционные системы реализуют очень слабые политики паролей (или вообще не применяют политики, основанные на односимвольных экземплярах), где, как минимум, должны быть надежные минимальные критерии.

3. Исследование фрагментов

Во многих операционных системах информация, уничтоженная пользователем, физически не уничтожается, а помечается как уничтоженная. Отныне его можно восстанавливать и использовать с помощью специальных инструментов. Основными источниками поиска в данной ситуации выступают дампы памяти, корзина компьютера, резервные копии файловой системы и много другое.

4. Превышение полномочий

При реализации атак, используя данный метод, злоумышленники ищут и используют ошибки политики безопасности программного обеспечения. Он уполномочен сверх того, что ему дали в соответствии с политикой безопасности. Обычно это достигается путем запуска программы от имени другого пользователя с необходимыми привилегиями или в виде системной программы (драйверы, службы и т. д.). Замена динамически загружаемых библиотек, используемых системной программой, или изменение переменных среды, описывающие путь к таким библиотекам, позволяет добиться хакерам нужной цели.

Определение защищенной операционной системы

Операционная система может быть названа с некоторой защитой, если она обеспечивает защиту от основных типов угроз, перечисленных выше. Защищенная операционная система должна включать средства для ограничения доступа пользователя к этому ресурсу и средства для аутентификации пользователя, который начинает работать в этой операционной системе. Кроме того, защищенная операционная система должна включать меры по предотвращению случайного или преднамеренного выхода из строя операционной системы.

Подсистемы защиты ОС и их функции.

Основные функции:

1. Пользователи системы могут получить доступ только к тем объектам операционной системы, доступ к которым разрешен в соответствии с текущей политикой безопасности.

2. Идентификация и аутентификация. Пользователи не могут запускать операции операционной системы, не идентифицируя себя и не предоставляя им информацию для аутентификации, чтобы убедиться, что они являются теми, кем себя называют.

3. Аудит. Операционная система регистрирует потенциально опасные события в специальном журнале для обеспечения безопасности системы. Записи этих событий могут быть просмотрены только администратором операционной системы в будущем.

4. Управление политикой безопасности. Политику безопасности всегда следует поддерживать в соответствующем состоянии. Политики безопасности управляются системным администратором с использованием соответствующих инструментов, встроенных в операционную систему.

5. Криптографические функции. В настоящее время информационная безопасность не может рассматриваться как не использующая средства криптографической защиты. В операционной системе шифрование используется для хранения и передачи пользовательских паролей и других данных, которые важны для безопасности системы по каналу связи.

6. Функция сети. Современные операционные системы, в принципе, не функционируют отдельно и функционируют как часть локальной и / или глобальной компьютерной сети. Операционные системы компьютеров в одной сети взаимодействуют друг с другом для решения различных задач, в том числе, непосредственно связанных с информационной безопасностью. Подсистема безопасности почти никогда не является единым программным модулем. В принципе, каждая из перечисленных функций подсистемы защиты разрешается одним или несколькими программными модулями. Некоторые функции встроены непосредственно в ядро операционной системы. Тем не менее, должен быть четко определенный интерфейс между различными модулями подсистемы безопасности, используемыми во взаимодействии модулей для решения общих проблем.

ОПЕРАЦИОННЫЕ СИСТЕМЫ, РЕАЛИЗУЮЩИЕ КОНЦЕПЦИИ ВИРТУАЛЬНОЙ МАШИНЫ НА ТЕЛЕФОННЫХ УСТРОЙСТВАХ

Дьяченко Николай Игоревич, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Стековая и регистровая архитектура виртуальной машины и Dalvik VM

Виртуальная автомат (VM) это абстракция над уровнем операционной системы, с помощью которой возможно эмулировать реальную машину. При помощи виртуальной машины можно запускать одну и ту же платформу под разными операционными системами и аппаратными архитектурами. Интерпретаторы Java и Python возможно рассматривать как примеры, в коих код компилируется в особый для их виртуальных машин байт код. Тоже самоеможно пронаблюдать и в архитектуре Microsoft .Net, где код компилируется в промежуточный язык для CLR (CommonLanguageRuntime).

Собственно, чтообязановходить в реализацию виртуальной машины? Она обязана эмулировать операции реальногомикропроцессора, и как эталон, содержатьследующие концепции:

- компиляция начального кода в особый для предоставленной виртуальной машины байткод
- стек вызовов для выполнения операций в функции
- структуры данных для содержанияинструкций и операндов (процесс обработки и данные)
- “указатель инструкции” (IP) указывающий на следующию выполняемую инструкцию
- виртуальный ЦП – обрабатывающего инструкции
- доставляемые указателем инструкции
- декодирование операндов
- выполнение инструкции

Есть два ведущих метода реализации виртуальной машины: стековый и регистровый. Образчик стековой виртуальной машины – виртуальная машина Java, Net CLR, это обширно применяемый способ реализации виртуальной машины. В качестве регистровой виртуальной машины возможно именовать Lua VM и Dalvik VM (которую мы коротко рассмотрим). Разница междaнными2-мяподходами в механизме, применяемом для записи и получения операндов и итогов исполнения команд.

Стековая виртуальная машина

Стековая виртуальная машинавыполняетглавные, выше описанные качества виртуальной машины, но в качестве структуры данных, куда помещаются операнды, применяется стек. Операции получают данные из стека, обрабатывают их и вносят в стек итог по правилу LIFO (последний пришел, 1-ый ушел).

Превосходство стековой модели в том, собственно, что операнды задаются неявно указателем стека (на рисунке – SP). Это значит, собственно, что виртуальной машине не надоявноуказывать на адреса операндов, указатель стека показывает на грядущий операнд. В стековых виртуальных машинах все арифметические и логические операции производятсяпри помощи получения операндов и возврата итогов в стек.

Регистровые виртуальные машины

Команды в регистровой виртуальной машине производятсябыстрее, чемподобные команды стековой виртуальной машины.

Другое превосходство регистровой модели, что,собственно, с помощью нее возможно выполнить оптимизацию, которая не имеет возможность быть исполнена при стековом подходе. К примеру,некоторое количество разодин встречающееся выражение при регистровом подходеимеет возможность быть вычислено лишь один раз и сохранено в регистре для дальнейшегоприменения, собственно чтосберегает время важное для пересчета выражения.

Но с иной стороны в среднем инструкция регистровой машины длиннее, чем в стековой машине, так как в ней тредуется очевидное директива операндов.

Виртуальная машина DALVIK

DALVIK – реализованная гугл виртуальная машина для Андроид и выполняющая функцию интерпретатора java кода на устройствах под управлением данной операционной системы. Для выполнения процесса Андройд делает отдельный экземпляр виртуальной машины. Это понижает возможность краша системы при падении 1-го из приложений. Dalvik реализует регистровую модель и в противовес обычного java байт кода, который делает 8 битные инструкции на стековой JVM, пользуется 16 битными инструкциями. Регистры реализованы в Dalvik в виде 4 битных полей.

В случае если мы желаем получить болеедетализированную информацию о том, как процесс получает экземпляр виртуальной машины, мы обязаны начать рассмотрение с этапа загрузки ядра Linux в Android:

При загрузке системы, загрузчик ОС загружает ядро в память и инициализирует системные характеристики. В скором временипосле этого:

- ядро запускает инициализирующую программу, которая считается родительским процессом по отношении ко всем иным процессам.

- инициализирующая программа запускает системные программы daemonи довольно значительный сервис "Зиготу" (процесс Zygote в основном загружает виртуальную машину при запуске системы).

- процесс зиготы делает экземпляр Dalvik, являющийся основоположником всех экземпляров Dalvik в системе.

- процесс зиготы например же запускает BSD сокет, который прослушивает входящие запросы.

- при получении еще одного запроса на создание свежего экземпляра Dalvik VM, процесс зиготы разветвляет родительский Dalvik VM процесс и передает дочерний процесс запрашивающему приложению.

Это короткое описание, как формируется и применяется виртуальная машина Dalvik в ОС Android.

Вернувшись к теме виртуальных машин, Dalvik выделяется от обыкновенной виртуальной машины Java тем, собственно, что она выполняет байткод Dalvik, который отличается от простого java байткода. Промежуточный шаг меж Java компилятором и Dalvik VM, на котором случается переустройство Java байткода в байткод Dalvik берет на себя DEX компилятор.

DEX компилятор конвертирует .class файлы java в .dex файлы, которые имеют меньший размер и оптимизированы для Dalvik VM.

В заточение хотелось бы сказать, что невозможно заявить, собственно, что стековая виртуальная машина более хороша, чем регистровая или же напротив, регистровая лучше стековой. Данный вопрос остается дискуссионным и очень занимательной областью для изучений.

Список использованных источников

1. Указ Президента РФ от 21.12.2016 N 699 (ред. от 25.12.2019) "Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации";
2. Приказ МВД России от 31 декабря 2019 г. N 995 "Об утверждении Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом (загранаппарате Министерства внутренних дел Российской Федерации)"
3. Федеральный закон "О полиции" от 07.02.2011 N 3-ФЗ
4. Указ Президента РФ от 01.03.2011 N 248 (ред. от 13.07.2020) "Вопросы Министерства внутренних дел Российской Федерации" (вместе с "Положением о Министерстве внутренних дел Российской Федерации")
5. Указ Президента РФ от 11.07.2004 N 865 (ред. от 17.09.2020) "Вопросы Министерства иностранных дел Российской Федерации"
6. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)
7. Глава 2 Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом: приложение к приказу МВД России от 31.12.2019 № 995

МЕТОДЫ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ В ИНТЕРНЕТЕ

Дякив Александр Степанович, курсант 2-ого курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Современные методы аутентификации позволяют осуществить подходящей конфигурации с учетом различных требований, к примеру, интернет-банк
использует двухфакторную аутентификацию, отдельные сервисы государственных услуг применяют помимо постоянного и временного пароля, еще и документ,
подтвержденный электронной цифровой подписью. В представленной статье раскрыты
основные методы аутентификации, применяемые в настоящее время планируемые для использования на ближайшую перспективу.

Аутентификация - Процедура проверки достоверно убедиться в том, что субъект, предъявивший свой идентификатор, на самом деле
является именно тем субъектом, идентификатор которого он использует. Для этого он
должен подтвердить факт обладания некоторой информацией, которая может быть доступна только ему одному (пароль, ключ и т.п.). Аутентификация требуется при доступе к таким интернет сервисам, как:

- электронная почта
- веб-форумы
- социальные сети
- интернет-банкинг
- платежные системы
- корпоративные сайты
- интернет-магазины

1. Классификация методов аутентификации

В зависимости от степени доверительных отношений, структуры, особенностей сети и удаленности объекта проверка может быть односторонней или взаимной. Также различают однофакторную и строгую (криптографическую) аутентификации. Из однофакторных систем, наиболее распространенными на данный момент являются парольные системы аутентификации. У пользователя есть идентификатор и пароль, т.е. секретная информация, известная только пользователю (и возможно - системе), которая используется для прохождения аутентификации. В зависимости от реализации системы, пароль может быть одноразовым или многоразовым. Рассмотрим основные методы аутентификации по принципу нарастающей сложности.

1.1. Базовая аутентификация

При использовании данного вида аутентификации имя пользователя и пароль включаются в состав веб-запроса (HTTP POST или HTTP GET). Любой перехвативший пакет, легко узнает секретную информацию. Даже если контент с ограниченным доступом не слишком важен, этот метод лучше не использовать, так как пользователь может применять один и тот же пароль на нескольких веб-сайтах. Опросы Sophos показывают, что 41% в 2006 г. и 33% в 2009 г. пользователей применяют для всей своей деятельности в Интернете всего один пароль, будь то сайт банка или районный форум [1] [2]. Также из недостатков парольной аутентификации следует отметить невысокий уровень безопасности – пароль можно подсмотреть, угадать, подобрать, сообщить посторонним лицам и т.д

1.2. Аутентификация по предъявлению цифрового сертификата

Механизмы аутентификации с применением цифровых сертификатов, как правило, используют протокол с запросом и ответом. Сервер аутентификации отправляет пользователю последовательность символов, так называемый запрос. В качестве ответа выступает запрос сервера аутентификации, подписанный с помощью закрытого ключа пользователя. Аутентификация с открытым ключом используется как защищенный механизм аутентификации в таких протоколах как SSL, а также может использоваться как один из методов аутентификации в рамках протоколов Kerberos и RADIUS.

1.3. Аутентификация по Cookies

Множество различных сайтов используют в качестве средства аутентификации cookies, к ним относятся чаты, форумы, игры. Если cookie удастся похитить, то, подделав его, можно аутентифицироваться в качестве другого пользователя. В случае, когда вводимые данные плохо фильтруются или не фильтруются вовсе, похитить cookies становится не очень сложным предприятием[3]. Чтобы как-то улучшить ситуации используется защита по IP-адресу, то есть cookies сессии связываются с IP-адресом, с которого изначально пользователь авторизовывался в системе. Однако IP-адрес можно подделать используя IP-спуфинг, поэтому надеяться на защиту по IP-адресу тоже нельзя. На данный момент большинство браузеров [4] используют куки с флагом HTTPonly [5], который запрещает доступ к cookies различным скриптам.

1.4. Децентрализованная аутентификация

Одним из главных минусов таких систем является то, что взлом дает доступ сразу ко многим сервисам

1.5. Отслеживание аутентификации самим пользователем

Во многом безопасность пользователей в Интернете зависит от поведения самих пользователей. Так например, Google показывает с какого IP адреса включены пользовательские сессии, логирует авторизацию, также позволяет осуществить следующие настройки:

- передача данных только по HTTPS.
- Google может детектировать, что злоумышленник использует ваш аккаунт (друзья считают ваши письма спамом, последняя активность происходила в нехарактерное для вас время, некоторые сообщения исчезли ...)[17]
- отслеживание списка третьих сторон, имеющих доступ к используемым пользователем продуктам Google

Зачастую пользователю сообщается с какого IP адреса он последний раз проходил аутентификацию.

1.6. Многофакторная аутентификация

Для повышения безопасности на практике используют несколько факторов аутентификации сразу. Однако, при этом важно понимать, что не всякая комбинация нескольких методов является многофакторной аутентификацией. Используются факторы различной природы:

- Свойство, которым обладает субъект. Например, биометрия, природные уникальные отличия: лицо, отпечатки пальцев, радужная оболочка глаз, капиллярные узоры, последовательность ДНК.
- Знание - информация, которую знает субъект. Например, пароль, пин-код.
- Владение - вещь, которой обладает субъект. Например, электронная или магнитная карта, флеш-память.

В основе одного из самых надёжных на сегодняшний день методов многофакторной аутентификации лежит применение персональных аппаратных устройств - токенов. По сути,

токен – это смарт-карта или USB-ключ. Токены позволяют генерировать и хранить ключи шифрования, обеспечивая тем самым строгую аутентификацию.

Использование классических «многоразовых» паролей является серьёзной уязвимостью при работе с чужих компьютеров, например в интернет-кафе. Это подтолкнуло ведущих производителей рынка аутентификации к созданию аппаратных генераторов одноразовых паролей. Такие устройства генерируют очередной пароль либо по расписанию (например, каждые 30 секунд), либо по запросу (при нажатии на кнопку). Каждый такой пароль можно использовать только один раз. Проверку правильности введённого значения на стороне сервера проверяет специальный сервер аутентификации, вычисляющий текущее значение одноразового пароля программно. Для сохранения принципа двухфакторности аутентификации помимо сгенерированного устройством значения пользователь вводит постоянный пароль.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЛИЧНОСТИ В СОВРЕМЕННОМ МИРЕ

Жигарев Максим Сергеевич, командир отделения 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Действительно, «кто владеет информацией, тот владеет миром». Владение ей в нужном объеме помогает человеку правильно оценить происходящие события, грамотно проанализировать ситуацию и на данной основе принять какое-либо правильное решение.

Поэтому в современном мире информация представляет собой ценность, которая является неким «посредником» при взаимодействии людей. Она настолько плотно вошла в нашу жизнь, что, не владея ей, человеку просто трудно функционировать в современном обществе.

Вследствие этого, каждый современный человек погружен в информационную среду, которая представляет собой набор условий для переработки и эффективного использования знаний в виде информационного ресурса. В процессе своей деятельности человек активно взаимодействует с информационной средой, в результате чего получает новые знания, анализирует их и представляет в виде информации опять же в информационной среде. Размещенная информация может быть как публичного характера, так и личного.

Информация в современном обществе может представлять собой сильное средство воздействия на личность. Следовательно, встает вопрос об обеспечении ее информационной безопасности. Под информационной безопасностью понимается защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных.

Но «состояние защищенности» зачастую неустойчиво. Современное общество все более нуждается в механизмах фильтрования информации и средствах защиты от нежелательной или недостоверной информации, так как практически каждый человек сталкивается с информационной угрозой.[1]

Общепринято определено, что под угрозой информационной безопасности понимается совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Опасность возникает как в отношении общества, государства, так и личности.

В настоящее время в информационной сфере встречается множество угроз. Это могут быть вторжение в частную жизнь, использование объектов интеллектуальной собственности, искажение информации, ограничение доступа к информации, хищение информации.

Проблема хищения информации является весьма актуальной в современном мире, так как ее касается почти каждый человек в виду столкновения с проявлениями данной проблемы: несанкционированным доступом к документам и файлам, хищением компьютеров и носителей информации, уничтожением информации, хищением логина и пароля и т. п.

Для анализа представленной проблемы мы провели социологический опрос. В нем участвовала молодежь в возрасте 17-22 лет. Это студенты высших профессиональных и средних профессиональных учебных заведений с различным профилем подготовки: экономика и управление, правоохранительная деятельность, менеджмент, технология и экономика, юриспруденция, технические системы в агробизнесе, сестринское дело. Более активными участниками опроса были девушки – 74% респондентов.

В результате опроса выяснилось, что основными источниками угроз информационной безопасности по мнению молодежи являются сеть Интернет и мобильный телефон, которые заняли очень значительную роль в жизни каждого человека. Большинство участников опроса

(90%) признались, что каждый день проводят время в сети Интернет и очень часто пользуются мобильным телефоном.

Так как сеть Интернет и мобильный телефон наиболее востребованы в использовании, мы попытались выяснить почему. Мы задались вопросом: «Для каких целей они чаще всего используются?» 68% опрошенных признались, что используют Интернет в основном для личных целей (электронная почта, социальные сети и т. д.), а также для учебной деятельности (28%) и работы. Мобильный телефон же используется для звонков (80% опрошенных), социальных сетей (78%), поиска в сети Интернет (64%), SMS (48%) и др.

Можно сделать вывод, что мобильный телефон и сеть Интернет в основном используются для доступа к социальным сетям, которые являются уязвимым кладезем личных данных.

Большинство респондентов (68%) солидарны в том, что угрозе информационной безопасности чаще подвергаются личные данные.

Но сначала мы захотели выяснить, знает ли вообще аудитория, что такое «информационная безопасность». А также поинтересовались мнением респондентов о том, как часто они встречаются с информационными угрозами и обеспечена ли их информационная безопасность.

Большинство участников опроса (62%) уверяют, что знают, что такое «информационная безопасность личности», или по крайней мере слышали данное определение в СМИ (24%). Остальные участники не осведомлены, что скрывается под этим понятием.

Респонденты утверждают, что встречаются с угрозой информационной безопасности в основном один раз в полгода или один раз в год (34% и 36%). Другая часть опрошенных признались, что встречаются с «угрозой» чаще: один раз в месяц (16%) или каждый день (14%).

Большинство опрошенных не могли определенно сказать, обеспечена ли их информационная безопасность (48%). Остальные участники опроса разделились на два противоположных мнения: 26% - уверены в своей информационной защите и 26% - определенно нет.

Таким образом, можно сделать вывод, что большинство представителей современного общества не осведомлены в области информационной безопасности. Есть люди, которые даже не имеют представления о данном понятии. Следовательно, они и не представляют, какой уровень защищенности их личных данных.

Но в результате исследования выяснилось, что аудитория хорошо осведомлена в том, какие угрозы информационной безопасности чаще подстерегают ту или иную личность. По мнению респондентов это спам (76%), вирусные атаки (66%), хищение логина и пароля (62%), использование телефона другими лицами (18%), хищение персональных данных (14%), несанкционированный доступ к персональному компьютеру (10%), хищение средств с платежной карты (6 %).

Поэтому наиболее популярными средствами от информационных угроз у личности, по мнению респондентов, являются программные средства защиты: антивирусы (90%), антиспамовые фильтры (22%), безопасные чаты (20%), межсетевые экраны (10%) и шифровальные подписи(6%). Остальная часть опрошенных призналась, что вообще не использует никакие средства защиты.[3]

На основе мнения участников опроса и проанализированных данных можно сделать вывод, что проблемы, связанные с обеспечением информационной безопасности личности являются актуальными в современном мире. Актуальность проявляется в том, что личность периодически встречается с угрозой информационной безопасности. И тому множество причин. По мнению респондентов это спам, выражающийся в угрозе информационному статусу личности, то есть в нарушении ее юридически закрепленного положения в информационном обществе. Большинство участников опроса видят угрозу в незаконном использовании сторонними лицами их личных данных как через хищение логина и пароля от

страницы в социальной сети и электронной почты, несанкционированный доступ к компьютеру и мобильному телефону, так и через вирусные атаки.

Отсюда следует вопрос о всесторонней безопасности личности от информационных угроз, что является одной из главных функций государства. Она предполагает правовое обеспечение информационной безопасности личности, которая включает: защиту чести, достоинства и деловой репутации граждан; защиту духовного и интеллектуального развития личности; защиту от недостоверной, негативной и недоброкачественной информации, дезинформации; защита информационных ресурсов и средств связи от несанкционированного воздействия сторонних лиц; защиту информационных прав и свобод личности в информационной среде.[4]

То есть защита информационной безопасности личности может реализовываться по двум направлениям: правовой защите и технической защите.

Согласно В.И. Ярочкину, первое направление предполагает специальные правовые акты, правила, процедуры и мероприятия по обеспечению защиты информации на правовой основе. Защита на государственном уровне реализуется применением правовых актов и норм права, надзором за их соблюдением, а также влечением наказания за их нарушение. Сюда включается осуществление положений Конституции РФ, законов РФ, гражданского, административного, уголовного права по реализации обеспечения информационной безопасности личности.

Второе направление безопасности личности в информационной сфере подразумевает использование технических средств защиты. На практике выделяют физические, аппаратные, программные, криптографические и комбинированные средства обеспечения безопасности информации.

Физические средства защиты предполагают предупредительные меры, устройства, исключающие несанкционированное проникновение к конфиденциальной информации (охрана источников информации – например, сейфы).

Аппаратные средства – это электронные и механические устройства, препятствующие утечке информации (ограничение доступа, видеонаблюдение и т. д.).

Программные средства представляют собой использование специальных программ для сохранения целостности и конфиденциальности информации (идентификация, аутентификация, программы ограничения доступа, регистрация работы средств, оповещения о несанкционированных действиях и т. д.).

Криптографические средства представляют собой шифрование информации. Что же касается комбинированного способа обеспечения информационной безопасности, то он предполагает сочетание аппаратных, программных и криптографических средств защиты.[5]

Таким образом, проблема информационной безопасности личности является одной из самых насущных в современном обществе. Это обусловлено тем, что информация приобрела большую ценность в современном мире. Она является главным средством взаимодействия людей, но при этом играет двоякую роль. То есть информация, с одной стороны, выступает как необходимый ресурс для существования современного общества, а, с другой стороны, она может представлять угрозу для личности, выражающуюся в незаконном использовании ее конфиденциальной информации. Вследствие этого, как государство, так и сама личность должны реализовывать необходимые правовые и технические меры защиты информационной безопасности личности.

Список использованных источников

1. Информационный портал «Языки программирования Pascal и Delphi»/. Информационная среда [Электронный ресурс]. URL: http://www.maksakov-sa.ru/Elem_IT/Inf_sreda/ (дата обращения: 10.03.2017).

2. Информационный портал «Академик». Информационная безопасность [Электронный ресурс]. URL: http://dic.academic.ru/dic.nsf/ruwiki/8410 (дата обращения: 16.03.2017).

3. Информационный портал «Википедия». Угрозы информационной безопасности [Электронный
ресурс]. URL: https://ru.wikipedia.org/wiki/Угрозы_информационной_безопасности#cite_note-1 (дата обращения: 16.03.2017).

4. Гафарова Г.Г., Смелянская В.В. Информационная безопасность личности//Социосфера. 2012. С. 56-58.

5. Ярочкин В.И. Информационная безопасность: Учебник для вузов. М.: Акад. Проект, 2012. 544 с.

СОВРЕМЕННЫЕ ЗАЩИЩЕННЫЕ ОПЕРАЦИОННЫЕ СИСТЕМЫ

Забавин Максим Вадимович, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В последнее время развитие компьютерных технологий происходит с невероятной скоростью, и в скором времени, невозможно будет представить жизнь людей без персонального компьютера или мобильного телефона. Сами по себе данные устройства — это лишь набор микросхем, а от операционной системы уже зависит скорость и производительность работы. Перед тем как приобретать персональный компьютер или любую другую вычислительную технику, необходимо изучить ОС, чтобы в дальнейшем знать чем вы пользуетесь. Актуальность данной темы заключается в том, что необходимо изучить отдельно одни из самых популярных операционных систем Windows, Android и Mac OS.

Объектом изучения является изучение современных операционных систем (Windows, Android и Mac OS).

Предметом изучения является рассмотрение особенностей работы операционных систем Windows, Android и Mac OS.

Исходя из курса Средств Вычислительной Техники (СВТ), операционная система – это комплекс взаимосвязанных программ, предназначенных для управления ресурсами вычислительного устройства и организации взаимодействия с пользователем, это основа компьютера, без нее на экране монитора можно будет увидеть только черный экран. ОС является программным обеспечением, которое с одной стороны, выступает мостом между устройствами вычислительной системы и прикладными программами, а с другой для управления устройствами, эффективного распределения вычислительных ресурсов между вычислительными процессами и организации надёжных вычислений.

Операционная система Windows является относительно защищенной и надежной операционной системой. Это достигается за счет постоянной поддержки обновлениями, которые устраняют так называемые «дыры», позволяющие получить злоумышленнику доступ к информации, хранящейся на компьютере.

Защита в системе Windows состоит из следующих компонентов:

1.Процедура инициализации пользователя в системе. Она представляет собой процесс, который организует диалог с пользователем при входе. Некая интерактивная процедура, которая может позволить пользователю получить удаленный доступ к устройству.

2.Менеджер учета – система, управляющая данными пользователя или группы из пользователей.

3.Диспетчер доступа – проверка пользовательских прав на доступ к запрашиваемому объекту и проверке его действий.

ОС Windows является носителем графического интерфейса, в котором основными элементами являются Рабочий стол, окно, меню и Панель задач. ОС Windows – это так же интегрированная среда, под управлением которой могут работать не только специальные программы, разработанные для данной ОС, но и альтернативные программы, так же DOS-приложения. Windows так же имеет возможность реализации подключения новых внешних устройств и обеспечение их самонастройки (Plug and Play – «Включи и работай»).

Заходя на официальный сайт разработчика операционной системы Mac в раздел безопасность пользователя встречает надпись: «Технически продвинутое оборудование и софт обеспечивают более безопасный запуск приложений на вашем Mac, большую конфиденциальность в сети интернет и надежную защиту данных». Так же компания Apple

призывает своих пользователей своевременно обновлять операционную систему, утверждая то, что «с каждым обновлением защита вашего устройства на IOS становится еще безопаснее».

Все устройства на операционной системе Android включают в себя встроенную в систему защиту на аппаратном и сетевом уровне всех данных от утечки. Существует безопасная среда Trusted Execution Environment (TEE), в которой происходит, например, шифрование данных. К тому же, все приложения работают в изолированной среде, она в свою очередь ограничивает доступ стороннего программного обеспечения к информации, хранящейся на устройстве. Так же на устройствах присутствуют сервисы безопасности Google, которые помогают избежать угрозы при скачивании сторонних приложений и изменении настроек.

Google Play Protect – одна из самых распространённых в мире служб по обнаружению угроз, которая встроена во все устройства на данной операционной системе и сканирует около 50 миллиардов приложений на более чем 2.5 миллиардах смартфонах для обнаружения вредоносных программ. Служба Google Play Protect может автоматически удалять вредоносные приложения в рамках своей профилактической инструкции и использовать ее для улучшения поиска потенциально вредоносных программ.

Android использует многослойные средства защиты, чтобы обеспечить безопасность операционной системы. С каждой версией ОС Android становится все прочнее, чтобы иметь правильную защиту от текущих угроз, с которыми сталкиваются пользователи. Безопасность ОС Android предусматривает несколько аппаратных функций, которые обеспечивают надежную защиту устройства.

Android Keystore System - система Android Keystore является основой защиты данных на устройствах. Она хранит криптографические ключи в контейнере, что затрудняет извлечение их из устройства. Android KeyStore смягчает последствия несанкционированного использования ключевых материалов на Android-устройстве, заставляя приложения указывать разрешенное использование своих ключей, а затем применяя эти ограничения вне процессов приложений. Для устройств, которые допускают защищенный экран блокировки и поставляются с Android 7.0 или выше, KeyStore должен быть реализован в защищенном оборудовании. Это гарантирует, что даже в случае компрометации ядра ключи KeyStore не будут извлечены из защищенного оборудования.

Было исследовано три операционные системы: Android, Windows. Mac. В данные ОС в основном выполняют практические функциональные задачи. Выбор пал на них, так как они являются наиболее популярными среди остальных, и их уязвимости представляют наибольший интерес. Функции информационной безопасности, если они включены в дизайн, являются всего лишь расширениями к существующей функциональности в виде плагинов, компонентов, реализующих алгоритмы шифрования или надстройки архитектуры. Эти меры могут помочь улучшить общую информационную безопасность, но не могут гарантировать защиту от всех современных моделей угроз. Теперь, в эпоху интернета, вопросы кибербезопасности, связанные с используемыми устройствами, становятся актуальнее. Именно безопасность операционной системы определяет общий уровень кибербезопасности всей встраиваемой системы. К сожалению, вопросам информационной безопасности до сих пор не уделяется достаточного внимания при разработке операционных систем.

Большинство на стороне операционной системы Android, она является самой легкой и быстрой ОС сейчас на рынке. Для функционирования ОС Android, в отличие от Windows, не нужен очень мощный процессор, чтобы работать на оптимальном уровне. ОС Windows подойдет тем людям, которые нуждаются в мультимедийном плеере, а так же для тех, кому необходим не очень дорогой и не самый тяжелый в использовании компьютер для работы. Mac OS X - это вариант для людей, которые хотят работать на компьютере, не вникая в особенности системы. Идеально защищенной операционной системы попросту не существует. Чтобы обезопасить свое устройство от внешних угроз пользователь должен

всегда своевременно обновлять программное обеспечение и проводить профилактику системы.

МЕХАНИЗМ НЕЧЕТКОГО ЛОГИЧЕСКОГО ВЫВОДА

Зайцев Михаил Александрович курсант 1-го курса МосУ МВД России имени В.Я Кикотя

Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Система нечеткого вывода — это ключевой элемент системы нечеткой логики, основной задачей которой является принятие решений. Он использует правила «ЕСЛИ… ТОГДА» вместе с соединителями «ИЛИ» или «И» для рисования основных правил принятия решений. Понятие **нечеткого вывода**занимает важнейшее место в нечеткой логике Алгоритм Mamdani, Алгоритм Tsukamoto, Алгоритм Sugeno, Алгоритм Larsen, Упрощенный алгоритм нечеткого вывода, Методы приведения к четкости.

Используемый в различного рода экспертных и управляющих системах механизм нечетких выводов в своей основе имеет базу знаний, формируемую специалистами предметной области в виде совокупности нечетких предикатных правил вида:

П1: если *x*есть A_1, тогда *y*есть B_1,

П2: если *x*есть A_2, тогда *y*есть B_2,

……

$П_n$: если *x*есть A_n,тогда *y*есть B_n, где *x*— входная переменная (имя для известных значений данных), *y* — переменная вывода (имя для значения данных, которое будет вычислено); A и B — функции принадлежности, определенные соответственно на *x*и *y*.

Пример подобного правила

Если *x* — низко, то *y* — высоко.

Приведем более детальное пояснение. Знание эксперта A → B отражает нечеткое причинное отношение предпосылки и заключения, поэтому его можно назвать нечетким отношением и обозначить через *R:*

$R = A \rightarrow B$,

где «→» называют нечеткой импликацией.

Отношение *R*можно рассматривать как нечеткое подмножество прямого произведения $X \times Y$ полного множества предпосылок *X* и заключений *Y.*Таким образом, процесс получения (нечеткого) результата вывода B' с использованием данного наблюдения *A'* и знания A → B можно представить в виде формулы

$B' = A' \circ R = A' \circ (A \rightarrow B)$,

где «о» — введенная выше операция свертки.

1. *Нечеткость* (введение нечеткости, фазификация, fuzzification). Функции принадлежности, определенные на входных переменных применяются к их фактическим значениям для определения степени истинности каждой предпосылки каждого правила.

2. *Логический вывод.* Вычисленное значение истинности для предпосылок каждого правила применяется к заключениям каждого правила. Это приводит к одному нечеткому подмножеству, которое будет назначено каждой переменной вывода для каждого правила. В качестве правил логического вывода обычно используются только операции min(МИНИМУМ) или prod(УМНОЖЕНИЕ). В логическом выводе МИНИМУМА функция принадлежности вывода «отсекается» по высоте, соответствующей вычисленной степени истинности предпосылки правила (нечеткая логика «И»). В логическом выводе УМНОЖЕНИЯ функция принадлежности вывода масштабируется при помощи вычисленной степени истинности предпосылки правила.

3. *Композиция.* Все нечеткие подмножества, назначенные к каждой переменной вывода (во всех правилах), объединяются вместе, чтобы формировать одно нечеткое подмножество для каждой переменной вывода. При подобном объединении обычно используются операции max(МАКСИМУМ) или sum(СУММА). При композиции МАКСИМУМА комбинированный вывод нечеткого подмножества конструируется как поточечный максимум по всем нечетким подмножествам (нечеткая логика «ИЛИ»). При композиции СУММЫ комбинированный вывод нечеткого подмножества конструируется как поточечная сумма по всем нечетким подмножествам, назначенным переменной вывода правилами логического вывода.

4. В заключение (дополнительно) — *приведение к четкости* (дефазификация, defuzzification), которое используется, когда полезно преобразовать нечеткий набор выводов в четкое число. Имеется большое количество методов приведения к четкости, некоторые из которых рассмотрены ниже.

На практике в задачах, подобных рассмотренной, количество переменных может быть существенным, могут одновременно использоваться различные композиции нечетких выводов, сама схема выводов может быть многокаскадной. Общих методов решения подобных задач в настоящее время, по-видимому, не существует.

Нисходящие нечеткие выводы

Рассмотренные до сих пор нечеткие выводы представляют собой восходящие выводы от предпосылок к заключению. В последние годы в диагностических нечетких системах начинают применяться нисходящие выводы. Рассмотрим механизм подобного вывода на примере.

ВЛИЯНИЕ ДОЛИ ГБЖ В МЕТАЛЛОЗАВАЛКЕ НА КАЧЕСТВО СТАЛИ

Зимаков Роман Дмитриевич, студент 3 курса
Научный руководитель Гришина Светлана Сергеевна, преподаватель высшей, категории металлургического отделения
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Для получения качественной стали необходимо подбирать качественную шихту. Шихта состоит из различных компонентов, таких как металлошихта, шлакообразующие, науглероживатели, окислители. При выплавке стали на качество будет влиять именно металлическая часть шихты.

Основой металлошихты является металлический лом. Он делится на две категории: группа нелегированных (А) и легированных (Б) отходов.

Недостаток качественного лома при выплавке электростали, повышаемые требования к качеству выплавляемой стали вынуждают искать альтернативные виды железа, такие как металлизованные окатыши и горячебрикетированное железо.

Металлизованные окатыши являются удобным материалом для регулирования уровня содержания остаточных элементов в электростали и их применение - это перспективный способ получения стали с гарантированной степенью чистоты. Но использовать металлизованные окатыши при выплавки стали можно только в том случае, если производство этих окатышей включено в цикл предприятия, так как они имеют существенный недостаток. Они обладают таким свойством, как пирофорность, т.е. склонностью к самовозгаранию при хранении и транспортировке вследствие высокой пористости и развитой поверхности к вторичному окислению. В результате окисления снижается их металлургическая ценность[1].

Один из наиболее эффективных способов понижения чувствительности железа прямого восстановления к поглощению влаги и окислению – его горячее брикетирование. Железо прямого восстановления выгружается из печи в горячем состоянии и может частично или полностью сразу же быть подвергнуто горячему брикетированию. При этом происходит его значительное уплотнение с устранением неприятностей, обусловленных механическими напряжениями, окислением и разогревом его при транспортировке, хранении и перегрузках.

Горячебрикетированное железо относится к одному из видов металлизованного сырья и является перспективным материалом для получения электростали с высокой степенью чистоты[2].

Следует отметить, что использование данного сырья становится экономически привлекательным при замене им чугуна и дорогостоящего вида лома в металлошихте даже при ухудшении технологических показателей электроплавки. Точно известный однородный химический состав ГБЖ со стабильными свойствами позволяет снизить вероятность непопадания в заданный химический состав полупродукта при его производстве.

Среди основных преимуществ ГБЖ можно выделить:

- отсутствие примесей цветных металлов в ГБЖ;
- низкое содержание серы и фосфора в ГБЖ;
- точно известный однородный химический состав;
- высокая удельная насыпная;
- относительно низкая стоимость ГБЖ;
- при использовании ГБЖ в шихте снижается вероятность повреждения футеровки при завалке по сравнению с загрузкой тяжеловесным ломом;
- стабильный фракционный состав ГБЖ;

Основные преимущества использования такого сырья хорошо известны, но недостаточно широко освещаются в литературе отрицательные моменты от влияния ГБЖ на стойкость футеровки печи, а также отсутствуют стандартные приемы работы с таким сырьем. Отмечены разные, в том числе и противоречивые мнения о влиянии ГБЖ на технологические показатели электроплавки – расходы энергоносителей, шлакообразующих добавок, стойкость футеровки печи и другие показатели. Все это зависит от ряда факторов: конструкции ДСП, энерготехнологических режимов, характеристик ГБЖ, способа загрузки ГБЖ в печь и прочих[4].

Рассмотрим основные проблемы при использовании ГБЖ:

При плавке губчатого железа с разовой завалкой расход электроэнергии с увеличением его доли до 50 – 70% возрастает в большей степени, чем при непрерывной загрузке из-за ухудшения теплопередачи.

В ряде случаев при использовании добавки ГБЖ при выплавке стали в ДСП отмечено повышение расхода энергоносителей и шлакообразующих материалов. Это связано с наличием оксидов железа в ГБЖ и значительным содержанием оксида кремния, что приводит к образованию кислых шлаков. Отмечено также увеличение времени плавки и снижение выхода годного.

С ростом содержания пустой породы увеличивается расход энергии на плавление и перегрев шлака и незначительно снижаются затраты тепла на восстановление железа. Расчеты показывают, что затраты тепла на шлакообразование при повышении на 1 % пустой породы превышают затраты на восстановление при снижении степени металлизации на 1% примерно в 3 – 3,5 раза. Отсюда следует, что с позиций энергетики снижение содержания пустой породы в губчатом железе более эффективно, чем повышение степени металлизации. Энергетические потребности плавления окатышей при температуре ванны 1570 ºС примерно на 30 – 35% выше, чем лома. Они возрастают до 35 – 40%, если для лома принять температуру 1530ºС. Следовательно, применение металлизованных материалов взамен лома потенциально всегда связано с повышением, по крайней мере на 30%, потребностей в энергии[3].

Тем не менее, несмотря на ухудшение некоторых технологических показателей плавки, использование ГБЖ в металлошихте все равно остается экономически привлекательным.

Влияние добавки металлизованного сырья, в том числе ГБЖ, на энерготехнологические показатели плавки проявляется по-разному и зависит от разных факторов – способа загрузки ГБЖ в печь, конструкцией печи, ведения энерготехнологического режима, физико-химических характеристик ГБЖ и других.

Для анализа влияния доли ГБЖ в шихте на технологические показатели плавки использовали расчет шихты и материальный баланс плавки стали марки 38Г2Ф производимой в ЭСПЦ АО «ОЭМК». Для расчетов использовали долю металлизованных окатышей в шихте от 10 до 90% с шагом 10%. Результаты расчетов отражены в табл.1.

Таблица 1 - Технологические показатели плавки стали марки 38Г2Ф при различном содержании ГБЖ в металлозавалке (расчет на 100 кг)

Доля ГБЖ,%	Масса готовой стали, кг	Масса шлака, кг	Содержание серы (S) в стали, %	Выход годного металла
10	95,239	8,27	0,03	90,98
20	94,143	9,88	0,03	89,91
30	93,055	11,49	0,03	88,84
40	91,972	13,11	0,02	87,78
50	90,893	14,72	0,02	86,72
60	89,817	16,33	0,02	85,66
70	88,743	17,94	0,02	84,61

80	87,67	19,55	0,01	83,56
90	86,598	21,16	0,01	82,50

При увеличении доли ГБЖ с 10 до 90 % количество шлака в печи увеличивается с 8,27 до 21,16 кг на 100 кг металлозавалки, что отражается на расходе электроэнергии. Выход годного металла при увеличении доли до 90, снижается, но также снижается содержание серы в стали, что тоже немаловажно при выплавке качественной стали.

В итоге, учитывая все показатели, можно сделать вывод, что оптимальным содержанием ГБЖ в металлозавалке будет 50-70%.

Список использованных источников

4. Бигеев В.А., Основы металлургического производства: учебник / В.А. Бигеев, К.Н. Вдовин., В.М. Колокольцев – Санкт-Петербург: Издательство Лань-Трейд, 2017. - 616 с.

5. http://emchezgia.ru/plavkavotkrytyh/2_shihta.php. Шихта для выплавки стали и требования к ней.

6. Коростелев А.А., Съемщиков Н.С., Семин А.Е., Котельников Г.И., Мурзин И.С., Емельянов В.В., Колоколов Е.А., Белоножко С.С. Повышение стойкости футеровки ДСП при использовании ГБЖ в завалке. // Новые огнеупоры. - 2018. - № 3. С. 3 – 10.

7. Тимофеев Е.С., Кочетов А.И., Тимофеева А.С. ЗАВИСИМОСТЬ ДЛИТЕЛЬНОСТИ РАСПЛАВЛЕНИЯ ШИХТЫ ОТ ГБЖ В ЗАВАЛКЕ ПРИ ВЫПЛАВКЕ СТАЛИ В ДСП-150 // Фундаментальные исследования. – 2006. – № 11. – С. 37-38; URL: http://fundamental-research.ru/ru/article/view?id=6515 (дата обращения: 18.02.2021).

СРЕДСТВА ВИРТУАЛИЗАЦИИ

Золоторев Денис Владимирович, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В последнее время ряд компаний, работающих не только в ИТ-секторах, но и в других областях, серьезно сосредоточились на технологиях виртуализации. Домашние пользователи также уважали надежду и удобство платформы виртуализации, позволяя одновременно запускать несколько операционных систем в виртуальных машинах. На данный момент технологии виртуализации являются одними из наиболее перспективных оценок различных исследователей информационных технологий. Платформа виртуализации и инструменты управления быстро растут, периодически появляются новые игры, а также процесс загрузки крупных игр от небольших компаний, занимающихся разработкой программного обеспечения для платформы виртуализации, инструментов для повышения эффективности виртуальной инфраструктуры.

Между тем, многие компании еще не готовы инвестировать в виртуализацию, поскольку они не могут точно оценить экономические последствия внедрения этой технологии и не имеют достаточного количества квалифицированных кадров. Хотя многие западные страны уже имеют профессиональных консультантов, которые могут анализировать ИТ-инфраструктуру, готовить план виртуализации физических серверов компании и оценивать рентабельность проекта, в России таких людей очень мало. Наконец, в ближайшие годы ситуация изменится, и когда различные компании оценят преимущества виртуализации, будут специалисты, обладающие достаточными знаниями и описаниями для внедрения технологий виртуализации разного масштаба. На данный момент многие компании проводят только локальные эксперименты по использованию инструментов виртуализации, при базовом использовании бесплатной платформы.

К счастью, многие производители, помимо коммерческих систем виртуализации, также предлагают бесплатные платформы с ограниченной функциональностью, поэтому компании могут чудесным образом использовать виртуальные машины в производственной среде предприятия и одновременно оценивать возможность перехода на серьезные платформы.

Виртуализация-это процесс создания программного обеспечения (или виртуального) представления чего-либо, такого как виртуальные приложения, серверы, хранилища и сети. Это единственный и самый эффективный способ снизить стоимость ИТ-инфраструктуры, одновременно повышая эффективность и адаптивность для компаний всех размеров [1].

Виртуальная машина представляет собой изолированный программный контейнер, который работает с собственной операционной системой и приложениями, подобно физическому компьютеру. Виртуальная машина работает так же, как физический компьютер, и включает в себя собственную виртуальную оперативную память, жесткий диск и сетевой адаптер.

Виртуальная машина представляет собой программный контейнер, который связывает или" инкапсулирует " полный пакет виртуальных аппаратных ресурсов, а также ОС и все ее приложения в программном пакете.

Технологии виртуализации разного масштаба. На данный момент многие компании проводят только местные эксперименты по использованию инструментов виртуализации с базовым использованием бесплатной платформы.

К счастью, многие производители, помимо коммерческих систем виртуализации, также предлагают бесплатные платформы с ограниченной функциональностью, поэтому

компании могут чудесным образом использовать виртуальные машины в производственной среде предприятия и одновременно оценивать возможность перехода на серьезные платформы.

Основными функциями виртуальных машин являются: совместимость (виртуальные машины вместе со всеми стандартными компьютерами, виртуальная машина запускает свою собственную операционную систему и выполняет свои собственные приложения); изоляция (виртуальные машины полностью изолированы друг от друга, как если бы они были физическими компьютерами); инкапсуляция (виртуальная машина полнота охватывает компьютерную среду).

Виртуальные машины полностью не зависят от основного физического оборудования, над которым они работают [2].

Хост-операционная система - это операционная система, установленная на реальном оборудовании. В этой операционной системе программное обеспечение виртуализации установлено как обычное приложение.

Эмулятор виртуальной машины - это программное обеспечение, установленное на операционной системе хоста и состоящее из мониторов виртуальных машин и графической оболочки.

Монитор виртуальных машин представляет собой программу, обеспечивающую все взаимодействия между виртуальным и реальным оборудованием, поддерживающую работу одной или нескольких созданных виртуальных машин и установленных гостевых операционных систем. Графическая оболочка обеспечивает взаимодействие пользователя с приложением виртуальной машины, позволяя настраивать создаваемые виртуальные машины под свои нужды и управлять ее работой.

Гостевая операционная система – это операционная система, устанавливаемая на созданную виртуальную машину. В качестве гостевых операционных систем можно использовать Windows, Linux и др [3].

Рассмотрев выше сказанное, можно подвести итог: Виртуализация значительно упрощает ИТ-инфраструктуру, повышая производительность за счет оптимизации использования ресурсов, снижения затрат на техническое обслуживание и управление. Это радикально сокращает время строительства типичной инфраструктуры и рационально использует ИТ-ресурсы, как аппаратные, так и человеческие.

Важным моментом является создание постоянно функционирующей ИТ-инфраструктуры, защищенной от сбоев и устойчивой к стихийным бедствиям. Из-за грамотно построенной среды виртуализации происходит сокращение незапланированного простоя и абсолютное исключение запланированных перерывов для обслуживания сервера или хранилища данных. При этом все ИТ-услуги могут уйти от привязки к конкретному поставщику.

Для компаний на любом уровне и на любом этапе развития ИТ-инфраструктуры можно реализовать автоматизацию процесса так или иначе в связи с распределением вычислительных ресурсов для различных подразделений внутри компании или для своих клиентов.

Список использованных источников

1. https://www.vmware.com/ru/solutions/virtualization.html
2. https://www.stekspb.ru/blog/it/virtualizaciya/
3. https://www.ixbt.com/cm/virtualization-servers-free.shtml

ВВОДНЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ СПОСОБОВ ДОСТУПА И УПРАВЛЕНИЯ УДАЛЕННОГО КОМПЬЮТЕРА В СЕТИ

Иванов Артем Александрович, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В современном цифровом мире информационные технологии сопровождают человека на всех этапах его жизни. Цифровая среда предоставляет достаточно большой спектр возможностей ее использования как в личных, так и в рабочих целях. Ярким примером личного пользования может послужить возможность организации взаимодействия между людьми для личного общения, либо для управления той или иной отраслью работы для компаний и организаций и все эти возможности осуществимы без установления личного контакта между пользователями. При их осуществлении используется доступный каждому способ использования удаленного компьютера.

В настоящее время для использования удаленного компьютера, его управлением и доступом существует достаточно обширный набор инструментов и способов как в глобальной, так и в локальной сети.

Одними из основных целей использования данного способа подключения являются просмотр, управление рабочим столом удаленного компьютера (системное администрирование) или, например, выполнение таких действий как: организация аудио – видео конференций, обмен файлами, установка дополнительного программного обеспечения и т.п.

Примером данного способа, наиболее популярным, может быть обычное подключение пользователя к своему офисному ПК, используя свой домашний ноутбук, так же как и при использовании компьютера на работе, не лишая себя необходимого функционала. Таким же способом пользуются большое количество компаний и предприятий, используя его с теми же возможностями, которые существуют в реальности.

Преимущества и недостатки использования удаленного доступа

Среди преимуществ при пользовании данным способом можно выделить:

- *Экономия средств* – наиболее частое пользовании системой удаленного доступа предоставляет возможность ограничиться от больших трат на приобретение многочисленных и схожих по всем параметрам видов программного обеспечения (далее – ПО), так как есть возможность выбора одного инструмента из большого их количества, с необходимым функционалом и параметрами, которые можно использовать на одном компьютере. Еще стоит отметить, что при организации доступа к целевому компьютеру, используемый для этого аппарат может не иметь больших аппаратных характеристик, т.е. не иметь большую стоимость.
- *Безопасность и конфиденциальность данных* – вся необходимая для пользователя информация, какие-либо документы и файлы в основном хранятся в дата-центрах, которые должны отвечать всеми необходимым требованиям безопасности: например при соединений с удаленным сервером могут использоваться системы шифрования данных, также может использоваться резервное копирование данных, с помощью чего вероятность утери либо краж в большинстве случаев сведена к минимуму.
- *Гибкость* – данная характеристика наверняка будет наиболее важным аспектом при выборе организации удаленной работы, т.к. существует возможность выполнения задач из любого места нахождения и в любое время суток. Для этого только будет необходимо

наличие безопасного соединения с сетью и удаленным компьютером, компьютер самого администратора и установленное на обоих средствах программного обеспечения.

Несмотря на весомые преимущества при использовании данной системой организации управления компьютером существуют некоторые возможные недостатки:

- *Зависимость от подключения к сети* – система удаленного доступа напрямую зависима от быстрого и стабильного соединения с сетью. Только благодаря этому система сможет адекватно отвечать запросам пользователя. При отсутствии данных характеристик пользование системой становится недоступным.
- *Возможное снижение производительности* – несмотря на всё, характеристики целевого компьютера также могут повлиять на работу с использованием удаленного доступа. Например, если удаленный компьютер имеет слабые функциональные возможности либо большое число подключенных компьютеров, то есть вероятность столкнуться со снижением производительности или появлением взаимных помех при работе с ним.
- *Наличие простоя* – простой возможен при неправильной работе если работа сервера была неправильно организована либо он был некорректно настроен, т.е. отсутствие его бесперебойной работы для организации сети. При таких сбоях функционирование всей системы будет остановлено до момента восстановления сети.
- *Отсутствие навыков в работе с системой* – при администрировании пользователь должен обладать определенным набором навыков для оперативного реагирования на появление возможных проблем во время работы в системе.

В настоящем времени метод обеспечения удаленного управления компьютером и других аппаратных средств с каждым днем набирает популярность среди людей и организаций. Это становится наиболее используемым ввиду того, что существенно сокращается время при выполнении определенных задач и отмечается рост количества, при их выполнении. Этот метод становится намного удобнее нежели, когда приходится организовывать работу с каждым аппаратным средством и, вдобавок, обеспечивая еще свое присутствие «лицом к лицу» с ним.

МЕТОДИКА СБОРА ИНФОРМАЦИИ ИЗ СОЦИАЛЬНЫХ СЕТЕЙ

Илькевич Анна Константиновна, курсант 3-его курса
Научный руководитель Казанцев Владимир Иванович, преподаватель СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

С развитием технологий системы связи выросли с проводных до беспроводных устройств. Теперь стало проще общаться людямпо всему миру. Вопрос о расстоянии уже не является оправданием отсутствия связи. Интернет также вызвал большие изменения в формах коммуникаций, которые доступны и используются в настоящее время. Это привело к росту социальных сетей, что позволило без труда общаться и делиться своими мыслями со многими людьми одновременно. Легко обмениваться информацией, например изображениями, рекламными объявлениями, видео и текстовыми сообщениями. С момента создания социальные сети привлекают множество лиц, фирм, неправительственных организаций, различных учреждений. Есть миллионы пользователей, каждый из которых имеет разные цели для использования этих сетей. Для многих людей это воспринимается как развлечение, для кого-то это стало платформой для самореализации или развития бизнеса. Существует множество типов социальных сайтов, и пользователь уже сам выбирает тот, с которым ему удобно работать.

Сайты социальных сетей и социальные сети включают в себя все типы онлайн-социальных платформ, которые позволяют участникам обмениваться интересами и мнениями и многими другими социальными взаимодействиями. Использование этих платформ становится доминирующим среди всех целей использования интернета, и сегодня веб-контент часто имеет функцию для обмена различного рода информации в социальных сетях.

Таким образом, объемы оперативно значимой информации, циркулирующей в социальных сетях, увеличиваются с каждым днем. Сведения о лицах, событиях и обстоятельствах, представляющих интерес для решения задач оперативно-розыскной деятельности, концентрируются в многочисленных информационных ресурсах сети. В этих условиях необходимо понимать особенности проведения оперативно-розыскных мероприятий, которые позволяют выявлять такие сведения, которые открывают перед оперативными сотрудниками новые возможности в противодействии преступности.

На данный момент общественные сети существенно подчеркнули интерес к применению данных из социальных сетей в структуре МВД. Коллективное использование структурированных данных позволяет использовать общественной сети для решения многих задач МВД: борьбы с мошенничеством, доведение до самоубийства, педофилия и др.

В общественных сетях находится множество значимого материала для уголовных и административных дел, из которого возможно получить данные о интересах, предпочтениях и особенностях людей и компаний. Для этого нужно найти нужное нам лицо в каждом источнике, но на многих из них люди не регистрируются либо указывают малое количество сведений, а также ложных данных.

Сайты социальных сетей включают в себя все типы онлайн-социальных платформ, которые позволяют участникам делиться интересами и мнениями и многими другими социальными взаимодействиями. Использование этих платформ становится доминирующим среди всех целей использования Интернета.

В результате популярности социальных программ растет стремление к большему пониманию структуры и эффектов социальных сетей. Понимание того, как социальные сети формируются, меняются с течением времени и структурируются в целом, улучшит способность проектировать и создавать системы. К сожалению, существующие методы сбора данных для анализа социальных сетей, которые не предоставляют адекватных средств для

систематического сбора больших объемов. Для проведения информативного анализа необходимо собрать надлежащие данные. Вместе с тем существующие методы сопряжённые с определенными трудностями, такими, как неспособность осуществлять сбор данных как в широких масштабах (число социальных связей), так и в узких масштабах (подробная информация о каждой связи и характере самой связи) без чрезмерной нагрузки на пользователей. Исследователи выразили заинтересованность в преодолении этих и других общих проблем сбора данных с целью облегчения сбора более подробной информации о социальных сетях. Современные автоматизированные инструменты обследования социальных сетей пытаются решить некоторые из этих проблем с ограниченным успехом путем компьютеризации более ранних подходов к обследованию на основе пера и бумаги. Были разработали различные инструменты, чтобы улучшить способность собирать данные социальных сетей непосредственно от отдельных лиц. Этиинструменты позволяет собирать подробную информацию от большого количества людей в короткие сроки, позволяя пользователям визуально организовать свои социальные контакты.

Исследователи используют различные методы сбора данных, включая структурированные и полуструктурированные интервью, опросы, наблюдения и интеллектуальный анализ данных для сбора данных социальных сетей. Возможно, наиболее распространенным методом сбора данных является опрос, состоящий из вопросов, направленных на получение подробной информации о социальных связях респондента. В опросах используются различные методы запрашивания предложений, и предпринимается попытка найти баланс между требуемыми усилиями респондента ответить на вопросы и качеством и/или количеством собранных данных. Методы исследования являются:

1) Интервью - могут проводиться лично или по телефону, а также могут проводиться формально или неофициально, вопросы должны быть целенаправленными, четкими и поощрять открытые ответы.

2) Анкеты и опросы - ответы могут быть проанализированы количественными методами путем присвоения численных значений, которые соответствуют различным шкалам. Результаты, как правило, проще (чем качественные методы) для анализа. Анкеты и опросы можно сравнить и проанализировать.

3) Наблюдение - позволяет изучать динамику ситуации, частоту отсчета целевого поведения или другое поведение, в зависимости от того, что указано в потребностях оценки. Также может производить качественные (например, описательные данные) и количественные данные (например, частоту, среднее взаимодействий и время проведение в социальных сетях).

Исходя из данных методов, целью исследования рассматриваемых страниц будет состоять в сосредоточении внимания на тех сетях, которые определяются как веб-сервисы, которые позволяют людям создавать публичный или полуобщественный профиль в ограниченной системе, формулировать список других пользователей, с которыми они совместно используют соединение, а также просматривать и пересекать их с другими в системе.

Одним из перспективных направлений оперативного розыска в сети Интернет считается оперативно-розыскной мониторинг (интернет-мониторинг), представляемый всеохватывающую систему ОРМ, которые обеспечивают надзор за состоянием преступных процессов в сетевой общественной среде и основаны на применении средств и способов ОРД именно в сети, нацеленной на сбор, обработку и тест информации о явлениях преступного намерения. Воплощение мониторинга может основываться на использовании в сети всевозможных ОРМ (наведение справок, выборочный опрос, надзор и др.).

Объектами такого мониторинга могут быть все типы информационных ресурсов в социальных сетях. Ведущими вариантами мониторинга, способными гарантировать высшую интенсивность поступления оперативно-розыскной информации, считаются: а) автоматическая разведка сетевых ресурсов, содержащих запретную к распространению информацию; б) исследование сетевых ресурсов, связанных с работой криминальных

сообществ; в) надзор за закрытыми для совместного доступа пространствами сетевого общения преступных направлений.

С позиций оперативно-розыскной деятельности социальные сети могут рассматриваться как:

- технологическая информационная система, которая обеспечивает передачу, обработку и хранение какой-либо информации и представляет ее оперативному сотруднику с помощью особого инструментария информационного поиска (технологический подход);

- сложный социокультурный феномен, который формирует особенную среду для реализации определенных видов деятельности и проявления специфических общественных отношений (социологический подход).

В зависимости от того, какая оперативная задача стоит перед сотрудниками, продуктивными в итоге могут оказаться оба перечисленных выше подхода. Так, например, особенности технологической среды социальных сетейпрямым образом связаны со способами совершения ряда преступлений. С их помощью можно определить специфику следов преступной деятельности, выбор технических средств, которые применялись в процессе раскрытия преступления, методы добывания оперативно-розыскной информации в информационных потоках и т.п. Помимо этого, специфика нового вида социального пространства, которое сформировалось в социальных сетях, накладывает свой отпечаток на стратегию и тактику ОРД, тем самым создавая особые условия для осуществления ОРМ.

БИОМЕТРИЯ И БЕЗОПАСНОСТЬ

Командир отделения 2 курса 991 взвода, младший сержант полиции Казаков А.А. и Курсант 2 курса 992 взвода, рядовой полиции Качура В.В
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

В 2018 году в России вступил в действие закон о биометрической идентификации. В банках идёт внедрение биометрических комплексов и сбор данных для размещения в Единой биометрической системе (ЕБС). Биометрическая идентификация даёт гражданам возможность получать банковские услуги дистанционно. Это избавляет их от очередей и технически позволяет «посетить банк» в любое время суток. Удобства дистанционной идентификации по фотографии или голосу по достоинству оценили не только клиенты банков, но и киберпреступники. Несмотря на стремление разработчиков сделать технологию безопасной, исследователи постоянно сообщают о появлении новых способов обмана таких систем.

Так может, не стоит соглашаться на предложение приветливого операциониста пройти биометрическую идентификацию в отделении банка? Или всё-таки воспользоваться преимуществами новой технологии? В чём проблема?

У биометрической идентификации есть особенности, которые отличают её от привычной пары логин/пароль или «безопасной» 2FA:

1. Биометрические данные публичны. Можно найти фотографии, видео- и аудиозаписи практически любого жителя планеты Земля и использовать их для идентификации.
2. Невозможно заменить лицо, голос, отпечатки пальцев или сетчатку с той же лёгкостью, как пароль, номер телефона или токен для 2FA.
3. Биометрическая идентификация подтверждает личность с вероятностью, близкой, но не равной 100%. Другими словами, система допускает, что человек может в какой-то степени отличаться от своей биометрической модели, сохранённой в базе.

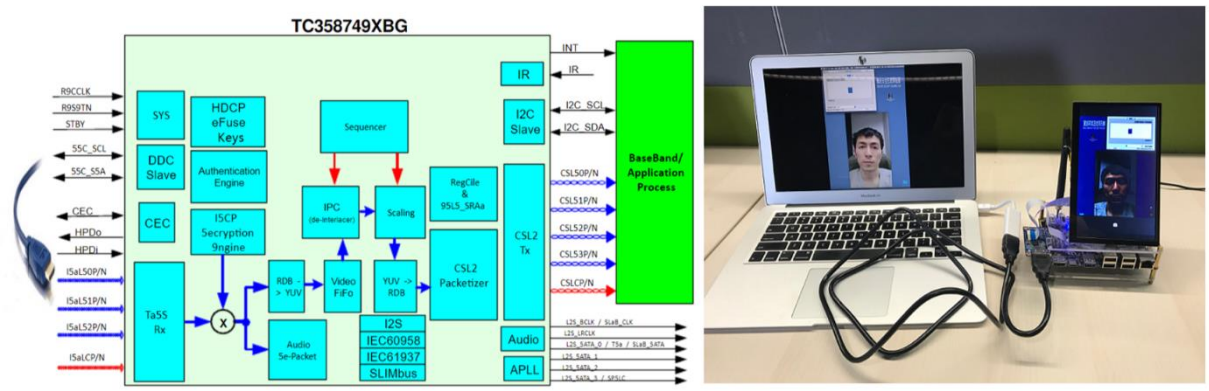
Поскольку биометрические данные открывают не только турникеты в аэропортах, но и банковские сейфы, хакеры и киберпреступники всего мира усиленно работают над способами обмана систем биометрической идентификации. Каждый год в программе конференции по информационной безопасности BlackHat неизменно присутствуют доклады, связанные с уязвимостями биометрии, но практически не встречается выступлений, посвящённых разработке методов защиты.

В качестве основных проблем, связанных с биометрической идентификацией, можно выделить фальсификацию, утечки и кражи, низкое качество собранных данных, а также многократный сбор данных одного человека разными организациями.

Публикации, связанные с различными способами обмана систем биометрической идентификации, часто встречаются в СМИ. Это и отпечаток пальца министра обороны Германии Урсулы фон дер Ляйен, изготовленный по её публичным фотографиям, и обман Face ID на iPhone X с помощью маски, нашумевшая кража 243 тысяч долларов с помощью подделанного нейросетью голоса генерального директора, фальшивые видео со звёздами, рекламирующими мошеннические выигрыши, и китайская программа ZAO, которая позволяет заменить лицо персонажа видеоролика на любое другое.

Чтобы биометрические системы не принимали фотографии и маски за людей, в них используется технология выявления «живости» — liveness detection — набор различных

проверок, которые позволяют определить, что перед камерой находится живой человек, а не его маска или фотография. Но и эту технологию можно обмануть.



Внедрение фальшивого видеопотока в биометрическую систему.

В представленном на BlackHat 2019 докладе «Biometric Authentication Under Threat: Liveness Detection Hacking» сообщается об успешном обходе liveness detection в Face ID с помощью очков, надетых на спящего человека, внедрения поддельных аудио- и видеопотоков, и других способов.

X-glasses — очки для обмана liveness detection в Face ID.

Для удобства пользователей, Face ID срабатывает, если человек надел солнцезащитные очки. При этом количество света в глазах уменьшается, поэтому система не может построить качественную 3D-модель области вокруг глаз. По этой причине, обнаружив

очки, Face ID не пытается извлечь 3D-информацию о глазах и представляет их в виде абстрактной модели — чёрной области с белой точкой в центре.

Качество сбора данных и ложные распознавания

Точность идентификации сильно зависит от качества биометрических данных, сохранённых в системе. Чтобы обеспечить достаточное для надёжного распознавания качество, необходимо оборудование, которое работает в условиях шумных и не слишком ярко освещённых отделений банков.

Дешёвые китайские микрофоны позволяют записать образец голоса в неблагоприятных условиях, а бюджетные камеры — сделать фото для построения биометрической модели. Но при таком сценарии значительно возрастает количество ложных узнаваний — вероятность того, что система примет одного человека за другого, с близким по тональности голосом или сходной внешностью. Таким образом, некачественные биометрические данные создают больше возможностей для обмана системы, которыми могут воспользоваться злоумышленники.

Многократный сбор биометрии

Некоторые банки начали внедрение собственной биометрической системы раньше, чем заработала ЕБС. Сдав свою биометрию, человек считает, что может воспользоваться новой технологией обслуживания в других банках, а когда выясняется, что это не так, сдаст данные повторно.

Ситуация с наличием нескольких параллельных биометрических систем создаёт риск, что:

- У человека, дважды сдавшего биометрию, скорее всего, уже не вызовет удивления предложение повторить эту процедуру и в будущем он может стать жертвой мошенников, которые будут собирать биометрию в своих преступных целях.
- Чаще будут происходить утечки и злоупотребления, поскольку увеличится количество возможных каналов доступа к данным.

Утечки и кражи

Может показаться, что утечка или кража биометрических данных — настоящая катастрофа для их владельцев, но, в действительности, всё не так плохо.
В общем случае биометрическая система хранит не фотографии и записи голоса, а наборы цифр, характеризующие личность — биометрическую модель. И теперь поговорим об этом подробнее.

Для построения модели лица система находит опорные антропометрические точки, определяющие его индивидуальные характеристики. Алгоритм вычисления этих точек отличается от системы к системе и является секретом разработчиков. Минимальное количество опорных точек — 68, но в некоторых системах их количество составляет 200 и более.

По найденным опорным точкам вычисляется дескриптор — уникальный набор характеристик лица, независимый от причёски, возраста и макияжа. Полученный дескриптор (массив чисел) и представляет собой биометрическую модель, которая сохраняется в базе данных. Восстановить исходное фото по модели невозможно
Для идентификации пользователя система строит его биометрическую модель и сравнивает с хранящимся в базе дескриптором.

СОВРЕМЕННЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калмыков Павел Юрьевич курсант 1-ого курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя»,
город Москва

Справедливо управлять всем интернетом нельзя, только Рунетом

Впервые за 16 лет президент Владимир Путин утвердил новую Доктрину информационной безопасности страны. Документ представляет собой «систему официальных взглядов на обеспечение национальной безопасности России в информационной сфере».

«Новая газета» взяла самые важные тезисы доктрины и спросила у экспертов о значении самого документа.

Что происходит с информационной безопасностью в мире (как это видят в Кремле):

Информационные технологии стали частью повседневной жизни и имеют глобальный характер. А если эффективно их использовать — можно ускорить экономическое развитие государства.

Чем опасен глобальный характер информации. Тем, что ее все чаще используются для достижения незаконных геополитических, военно-политических, а также террористических, экстремистских, криминальных целей в ущерб международной безопасности.

Воздействуя на информацию, можно вести войну нового поколения. Ряд зарубежных стран наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях.

Спецслужбы воруют гостайну, военные и научные секреты. Активизировались организации, специализирующиеся на технической разведке в отношении российских госорганов, научных организаций, предприятий оборонки.

Информационные атаки угрожают национальной безопасности. Спецслужбы отдельных государств оказывают «информационно-психологическое воздействие», чем пытаются дестабилизировать ситуацию в странах различных регионов мира, подорвать суверенитет и нарушить территориальную целостность уязвимых стран.

Интернетом нельзя управлять справедливо. Ресурсы, необходимые для безопасного и устойчивого функционирования интернета, распределены в мире неравномерно. Это означает, что управлять глобальным интернетом на принципах доверия и справедливости невозможно в принципе.

Кто и зачем угрожает России в информационном поле и где у нее слабые места (как их оценивают в Кремле)

Зарубежные СМИ увеличивают объем материалов, содержащих предвзятую оценку государственной политики России.

Российским журналистам за рубежом мешают заниматься профессиональной деятельностью.

Население России (а особенно — молодежь) зомбируют «в целях размывании традиционно российских духовно-нравственных ценностей».

Террористические организации воздействуют на отдельных людей и их группа, а также на все общество, нагнетая атмосферу межнациональной и социальной напряженности, а также вербуют новых сторонников.

Растет количество и масштаюы кибератак на кредитно-финансовую сферу.

Отдельные государства и организации применяют информационные технологии в военно-политических целях, направленных на подрыв суверенитета, политической и

социальной стабильности, территориальной целостности Российской Федерации и ее союзников

Усиливается разведывательная деятельность иностранных государств в отношении России.

Как Россия будет защищаться от угроз в сфере информационной безопасности

В области обороны:

будет сдерживать и предотвращвть военные конфликты, которые может спровоцировать применение информационных технологий.

будет совершенствовать систему информационной безопасности армии, причем не только защитного характера, но и атакующие силы («силы и средства информационного противоборства»).

будет защищать интересы союзников России в информационной сфере.

будет нейтрализовывать информационно-психологическое воздействие, направленного «на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества».

В области государственной и общественной безопасности:

будет противодействовать пропаганде экстремистской идеологии и средствам ее доставки.

будет пресекать деятельность спецслужб и организаций иностранных государств, бороться с их техническими средствами.

будет не допускать иностранный контроль над объектами информационной инфраструктуры.

будет заниматься профилактикой правонарушений, совершаемых с использованием информационных технологий.

будет защищать госутайну за счет существующих информационных технологий.

будет нейтрализовывать информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

В экономической сфере:

будет развивать отрасли информационных технологий с помощью поддержки инноваций, будет увеличивать доли этой отрасли в ВВП и структуре экспорта страны.

будет широко внедрять отечественные разработки.

будет повать конкурентоспособность российских компаний, действующих в отрасли информационных технологий.

В области науки и образования:

будет создавать информационные технологии, устойчивые к различным видам внешнего воздействия.

будет исследовать разрабатывать перспективные технологии и средства обеспечения информационной безопасности.

будет формировать культуру личной информационной безопасности.

В области стратегической стабильности:

будет проводить самостоятельную политику на реализацию национальных интересов в информационной сфере.

будет формировать системы международной информационной безопасности с партнерами.

будет продвигать позиции России на международном уровне, стремиться к взаимовыгодному и равноправному сотрудничеству стран, заинтересованных в информационной сфере.

будет развивать национальную систему управления российским сегментом сети интернет.

Заражение ПК не происходит при загрузке зараженного Web-сайта

То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов

"попутной загрузки" возможно уже на протяжении многих лет. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке".Во-первых, Web-сайты, созданные специально с целью заражения ПК.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое заражение ПК вредоносной программой. Преимуществом данного способа для киберпреступников является то, что им не приходится рекламировать Web-сайт. Для дальнейшей манипуляции данным Web-сайтом злоумышленникам необходимо в него внедриться. Если Web-сайт хорошо защищен, то осуществить такое внедрение очень сложно.

КВАНТОВЫЕ КОМПЬЮТЕРЫ

Каменев Павел Олегович, курсант 4-го курса
Научный руководитель Плотников Герман Геннадьевич, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

В обычных компьютерах с кремниевыми чипами информация хранится в двоичном коде, в битах. Это означает, что вычислительный элемент может дать одно из двух значений — 1 или 0, ‘true’ или ‘false’. Эквивалентом бита в квантовом компьютере является квантовый бит, или кубит. Чем больше число кубитов, тем выше вычислительная мощность конкретного квантового компьютера. Квантовый процессор, состоящий из кубитов, может находиться одновременно во всех возможных состояниях, но в каждом — с определенной вероятностью. Это явление, называемое квантовой суперпозицией, позволяет одновременно обрабатывать большие объемы данных и решать задачи, слишком сложные для обычных компьютеров. Вычислительный процесс представляет собой общесистемный переход, переводящий заранее определенный набор данных в некое новое состояние, которое и считается решением. В силу своей квантовой природы эти вычислительные элементы относительно нестабильны, и одной из главных инженерных задач является создание кубитов, которые прослужат как можно дольше. Не должно быть никакого влияния на квантовую систему, пока она работает, так как это потенциально может повлиять на результаты.

То, как работает квантовый компьютер, можно сравнить со знаменитым мысленным экспериментом "Кот Шредингера". Другим феноменом, лежащим в основе квантовых вычислений, является квантовая запутанность. Несколько объектов могут " синхронизировать’ свои квантовые состояния: когда состояние одного объекта изменяется, связанные с ним элементы мгновенно реагируют, изменяя свои состояния. Этот эффект не зависит от расстояния между объектами, а значит, квантовые компьютеры не будут иметь ограничений в скорости обработки информации. Более того, можно создать совершенно зашифрованный канал связи без каких-либо задержек.

Квантовые компьютеры предлагают совершенно новый подход к работе с информацией, не зависящий от скорости света или размера атома.

Современный уровень технического прогресса позволяет нам собирать огромное количество информации об окружающем нас мире. Однако современный уровень вычислительной мощности позволяет обрабатывать лишь малую часть данных, полученных, скажем, от Большого Адронного Коллайдера, астрономических обсерваторий или генетических лабораторий.

В области фундаментальных и прикладных наук квантовые вычисления, несомненно, могут уравновесить количество полученных необработанных данных со скоростью их обработки.

Тем не менее, несмотря на удивительные возможности, которые они предоставляют, квантовые технологии представляют собой ряд проблем, которые в основном вызваны принципиально иными законами природы и трудностями перехода к квантовой механике.

По сути, квантовые компьютеры делают устаревшими практически все современные подходы к программированию, обработке и защите данных. Человечеству придется не только освоить новые технологии, но и сосредоточиться на создании совершенно новых протоколов передачи данных и инфраструктуры.

Для крупных игроков на ИТ-рынке квантовые компьютеры представляют, как удивительный потенциал, так и огромные риски. Поскольку современные корпорации, такие как Google или Facebook, получают большую часть своих доходов от рекламы и продажи

пользовательских данных, они будут вынуждены полностью перестроить свои бизнес-модели, потому что существующие технологии просто перестанут работать.

Квантовые вычисления также вызывают значительный интерес на правительственном уровне. Новая компьютерная революция резко сократит влияние отдельных политиков, поскольку решения большинства правительственных проблем будут легко вычисляться. В то же время вопросы регулирования квантовых технологий будут решаться и на политическом уровне. Вопросы, связанные с координацией и законодательством квантовых компьютеров, могут возникнуть в ближайшем будущем — как только мы увидим первую машину с достаточной вычислительной мощностью, чтобы угрожать конфиденциальности личных, корпоративных или правительственных данных, или нарушать финансовые системы.

Современные квантовые вычислительные системы-это огромные сложные машины, разработка и обслуживание которых обходятся чрезвычайно дорого. Только корпорации или университеты могут себе это позволить. Но то же самое происходило и с обычными компьютерами, которые занимали целые комнаты и помещались на наших столах — и даже в карманах.

Полноценные квантовые компьютеры, вероятно, появятся в ближайшие пару десятилетий, но из-за высокой стоимости частные пользователи смогут арендовать только вычислительные мощности и облачные сервисы, подобные тем, которые сейчас предлагает IBM.

Станем ли мы когда-нибудь свидетелями создания миниатюрных квантовых смартфонов с мощностью, превосходящей все современные компьютеры, позволяющих передавать любую информацию в любую точку вселенной? Трудно сказать наверняка. Но практическое применение законов, действующих на квантовом уровне — совершенно отличных от тех, которые используются в нашем макромире, управляемом механическими законами Ньютона, — уже, кажется, находится в пределах нашей досягаемости.

ПРОГРАММЫ ВИЗУАЛИЗАЦИИ ПРИ ПРОИЗВОДСТВЕ ПРОКАТА

Ряполов Кирилл Игоревич, студент 3-го курса
Научный руководитель Комарова Юлия Викторовна, преподаватель 1 категории
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Исследования в 2011 году подтвердили, что мозгу легче обрабатывать картинки, чем текст. Когда мы смотрим на картинки, наш мозг может одновременно обрабатывать несколько элементов, поэтому визуализация — один из мощных и проверенных методов.

Визуализация техпроцесса - способ отображения информации о состоянии технологического оборудования и параметрах технологического процесса на мониторе компьютера или операторской панели в системе автоматического управления в промышленности, предусматривающий также графические способы управления техпроцессом. Визуализация процессов металлургии позволит упростить взаимодействие человека с машинами производства благодаря более понятному и интуитивному представлению техпроцесса, тем самым ускорив работу предприятия.

Актуальность темы заключается в исследовании возможности моделирования технологического процесса производства проката в системе визуализации и решении в виртуальной среде задач по повышению эффективности производства.

Целью исследования является ознакомиться с цифровой средой будущего и выявить эффективность внедрения систем визуализации на примере действующих систем.

Визуализация позволяет:

- представлять информацию в виде оптического изображения;
- размещать всю информацию о производственном процессе так, чтобы она была видна с первого взгляда;
- быстрое информирование персонала - при этом полученная информация доступна для дальнейшего использования;
- осуществление визуального контроля - позволяет отслеживать брак, проблемы в производстве и статус прохождения изделия по линиям в режиме реального времени.

Существуют следующие методы визуализации:

1. Метод цветового кодирования — указывает, для чего конкретно нужны те или иные детали, инструменты, приспособления.
2. Метод графических инструкций — для иллюстрирования операций и требований по качеству на каждом этапе производства и рабочем месте.
3. Метод информационных табличек — таблички могут быть статичными или электронными. Последние помогают в режиме реального времени следить за уровнем производства, дефектами и состоянием оборудования.

Черная металлургия - одна из отраслей промышленности, в которой вопросы автоматизации производства и управления традиционно имеют ключевое значение при решении задач повышения эффективности производства и обеспечения качества продукции.

Совершенствование систем автоматизации в металлургическом производстве связано с усложнением самих металлургических машин и реализуемых на них технологических процессов, а также с развитием приборостроения, техники электроприводов, электронной и вычислительной техники.

Основная задача прокатного производства состоит в обеспечении требуемого качества проката, т.е. обеспечении соответствия геометрических размеров, формы, физико-механических свойств и состояния поверхности проката заданным требованиям. Процесс производства проката осуществляется в несколько стадий, каждая из которых включает следующие основные технологические операции:

- подготовка металла к прокатке;
- нагрев металла перед прокаткой (при горячей прокатке);
- прокатка металла;
- отделка проката.

Благодаря внедрению визуализации производственный персонал будет лучше понимать стадии, которые проходит металл, а так же быстрее определять дефекты при выполнении работ и быстро устранять их в случае возникновения.

Основу системы составляет программное обеспечение (ПО). Оно состоит собственно из программы-визуализатора, которая устанавливается на рабочем месте и выполняет отображение сценария технологической операции в соответствии с установленной последовательностью действий, и программы — редактора сценария, которая используется при подготовке производства и устанавливается только на рабочем месте технолога.

Сначала, исходя из технологического процесса, определяются операции, которые должны быть визуализированы. Затем формируется список операций и переходов в порядке их выполнения. Для каждого перехода создается поясняющий текст. Далее определяется содержание каждой иллюстрации и готовятся файлы, которые будут использованы в качестве иллюстраций. На завершающем этапе с помощью программы-редактора файлы иллюстраций и тексты описаний включаются в сценарий.

Затем по сети файл сценария передается на рабочие места, где у каждого работника установлен экземпляр программы-визуализатора. Во время работы программа-визуализатор загружает этот сценарий и подключает к нему необходимые файлы иллюстраций и поясняющие тексты.

В простейшем варианте применения программа-визуализатор устанавливается на обычный компьютер рабочего места. При этом работник может легко и быстро увидеть пошаговую инструкцию по выполнению выбранной операции, здесь же в нужный момент ему будут предоставлены требования к материалам, инструменту, необходимые пояснения, спецификации, эскизы, схемы, чертежи — все, что технолог посчитает нужным внести в сценарий.

В более продвинутой реализации системы используется сенсорный монитор, который позволяет работать с ПО без применения клавиатуры и мыши. Все действия работник совершает через виртуальные кнопки на экране монитора. Кроме того, возможно применение малогабаритного системного блока компьютера и закрепление монитора на кронштейне над поверхностью рабочего стола. Все это позволяет полностью освободить пространство рабочего стола для производственных нужд.

Кроме того, иногда работники недостаточно хорошо знают технологию. Это решение позволяет в максимальной степени извещать специалиста о всех технологических тонкостях, на изучение которых у него нет времени.

Задача визуализации технологических операций востребована и со временем будет иметь огромное значение в производстве. Повсеместное внедрение автоматизированных информационных систем управления производством, которое сейчас активно происходит, позволяет объединить задачи визуализации технологии и фиксации производственных результатов в реальном времени. Результат этого внедрения сможет обеспечить минимизацию производственных ошибок, снижение влияния человеческого фактора в производственном процессе, реализацию прослеживаемости в производстве и совершенствование механизмов оперативного управления производством.

ДИСТАНЦИОННОЕ УПРАВЛЕНИЕ МОСТОВЫХ КРАНОВ

СоколенкоАнтон Романович, студент 3-го курс
Научный руководитель Сульдин Дмитрий Владимирович, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования
«Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Каждая успешная компания заинтересована в безопасности и эффективности своего производства. Управление грузоподъемным оборудованием в данном случае занимает существенную роль. С развитием технологических решений, предлагались новые системы и варианты управления крана. Уже сейчас, управление с кабины постепенно сменяется дистанционным. Дистанционное управление обеспечивает простоту контроля над краном, достаточный обзор рабочего пространства и, в то же время, безопасность оператора.

Актуальность темы учебного исследования заключается в необходимости упрощения эксплуатации оборудования по перемещению груза и увеличению безопасности операций на подъемно-транспортных механизмах.

Задачи учебного исследования:

1. рассмотреть виды дистанционного управления;
2. выявить особенности применения дистанционного применения;
3. рассмотреть материальные расходы при переводе на дистанционное управление;
4. определить экономическую выгоду применения дистанционного управления.

Благодаря универсальности дистанционного управления, подобный способ манипулирования ёширокоиспользуетсяна многих предприятиях. Дистанционная система управления краном повсеместно используется для козловых, мостовых, консольных кранов, а также МПУ и электроталей. Выделяют два вида дистанционного управления кранами:

- кнопочное;
- джойстиковое.

Кнопочное радиоуправление на данный момент является более распространенным. Для осуществления манипуляций краном оператор использует настроенные на необходимый механизм кнопки. В случае необходимости на одну кнопку механизма можно задать до 2-ух скоростей его передвижения (дополнительно сообщаем, что для возможности настройки более 1 скорости, механизм должен быть оснащен электрическим двигателем с двумя обмотками или оборудован преобразователем частоты.) Джойстиковое радиоуправление используется реже, в основном на площадках где скоростей у механизмов должно быть более 2-ух. Также в случае решения Заказчика о более удобном использовании в работе данного типа пульта. Пульт такого типа оператор не держит в руках, а закрепляет на шее с помощью специального ремня, для манипуляций краном используются специальные джойстики, настроенные на необходимый механизм. В случае необходимости на один джойстик механизма можно задать до 5-ти скоростей его передвижения (дополнительно сообщаем, что для возможности настройки более 1 скорости, механизм должен быть оборудован преобразователем частоты).[1]

Радиоуправление сейчас является наиболее современным вариантом контроля передвижения и манипулирования краном. Для радиоуправления необходимо осуществить подключение системы к цепи управления грузоподъемным механизмом. Важна готовность самого грузоподъемного оборудования к установке системы радиоуправления. При отсутствии пусковых резисторов (ступенчатого пуска двигателей) в схеме крана, дополнительно приобретается требуемое оборудование.

Преимуществами управления крановым оборудование при помощи радиоуправления является:

- возможность управлять краном с любой точки помещения;
- отсутствие дополнительных кабелей управления, кабины оператора;
- возможно управлять сразу несколькими кранами с одного пульта.

Установка радиоуправления начинается с проверки техдокументации грузоподъемного оборудования. Затем осуществляется осмотр крана и подбор комплекта радиоуправления. После согласования оптимальной системы выполняется установка радиоприемника в электрощитовую крана. Осуществляется настройка параметров крана, его проверка и последующее введение в эксплуатацию.

Перевод кранов на радиоуправление максимально целесообразен в следующих отраслях/сферах: промышленность, металлургия, возведение, горная индустрия. К каждой из сфер существует масса подъемного оборудования, которые можно перевести на радиоуправление. Производственники, строители, представители иных сфер весьма интересуются возможностью оптимизации затрат на содержание грузоподъемного оборудования, и увеличения его производительности.[2]

Радиоуправление состоит из радиоприемника, пульта-манипулятора (модуля управления краном) и блока передачи сигнала.

Радиоприемник. Приемник устанавливается в непосредственной близи от крана или на самом кране. С целью обеспечения безопасности работы и во избежание радиопомех при работе дистанционного управления применяется отдельный набор радиочастот.

Опционально, модуль радиоуправления можно снабдить обеспечением для ограничения зон работы крана и предотвращения попадания грузоподъемного оборудования в опасную зону.

Пульт управления. Радиус действия радиосигнала пульта в среднем составляет от 40 до 100 метров. Для удобства пульт радиоуправления можно крепить стационарно или на поясе/шее у оператора крана.

Как и для радиоуправления, так и для управления с пола применяются кнопочные, джойстиковые пульты. Простые кнопочные пульты имеют одну или две скорости. Более функциональные имеют до 5 скоростей и рычажные элементы управления с большим набором функций для управления краном.

Эксплуатация кранов с системой радиоуправления выполняется согласно с: «Типовой инструкцией крановщиков-операторов грузоподъемных кранов мостового типа, оснащенных радиоэлектронными средствами дистанционного управления РДИ7-75-96» Согласованной Госгортехнадзором России письмом № 12-7/181 от 04.03.96, с изменениями № 1 РДИ7-87 (75)-02, дополненными с учетом особенностей местных условий безопасной эксплуатации кранов и утвержденной руководителем данного предприятия.

Управление с пола представляет собой пульт на кабеле, который подводится непосредственно к грузоподъемному оборудованию.

К преимуществам можно отнести:

- Существенное улучшает производительность крана;
- Повышение безопасность эксплуатации кранового оборудования;
- Более точное позиционирование грузов, так как оператор наблюдает за перемещением груза в непосредственной близости;
- Снятие с учета в Ростехнадзоре при переводе крана с грузоподъемностью до 10 тонн на управление с пола (при демонтированной кабине оператора).

В п 9.1.11 правил ПБ 10-382-00 отмечено, что: Краны, не подлежащие регистрации в органах Госгортехнадзора, а также съемные грузозахватные приспособления снабжаются индивидуальным номером и под этим номером регистрируются их владельцем в журнале учета кранов и грузозахватных приспособлений.

Как и в случае с радоуправлением устанавливается и разрабатывается согласно требованиям регламентной документации, требований РД 24.090.90-89 (Машины

грузоподъемные Основные требования к техдокументации на реконструкцию). В этом документе предписывается исполнение работ специализированными организациями.

Согласно правилам ПБ 10-382-00 п. 9.1.3 не подлежат регистрации в органах Гостехнадзора краны мостового типа (мостовые, козловые, кран-балки) и консольные краны грузоподъемностью до 10 т включительно, управляемые с пола посредством кнопочного аппарата, подвешенного на кране, или со стационарного пульта.

После реконструкции крана (перевода на управление с пола), он переходит в разряд не требующих его регистрации (учета) в органах Ростехнадзора. Так в п. 9.2.6 сказано, что: Разрешение на пуск в работу кранов, не подлежащих регистрации в органах Госгортехнадзора, выдается инженерно-техническим работником по надзору за безопасной эксплуатацией грузоподъемных кранов на основании документации предприятия-изготовителя и результатов технического освидетельствования. При этом обязательна проверка всех команд управления и аварийных защит при работе крана в режиме управления краном с пола.

Для особых условий эксплуатации системы радиоуправления и управления с пола оснащаются дополнительной влаго- и пылезащитой, ударопрочным корпусом. Предусмотрена установка дублирующих систем, которые обеспечивают непрерывный процесс управления кранов в случае выхода из строя пульта. Также всегда возможно установить комбинацию радиоуправления и управления пультом на кабеле.

Принцип действия аппаратуры дистанционного управления краном

Сигнал, поступающий с пульта обрабатывается системой дистанционного управления, после чего на приемном узле осуществляется активация пусковых резисторов двигателя, которые приводят в движение кран. Возможности управления включают в себя контроль работы электромагнита, грейфера, освещения крана и других производственных элементов.

Дистанционное управление позволит:

- достичь оптимального обзора рабочей области;
- сэкономить электричество за счет сокращения холостых проходов крана;
- сократить персонал, работающем на кране - работу стропальщика и крановщика может выполнять один человек;
- повысить безопасность персонала,работающего в непосредственной близости от перемещаемого груза;
- снизить эксплуатационные расходы.[1]

Список использованных источников

1. Атлант Кран [Электронный ресурс]:https://atlant-kran.ru/article/114-ustrojstvo-sistem-upravlenija-kranami.html. Устройство систем управления кранами
2. UTING.[Электронный ресурс]:http://www.uting.ru/statji/plyusy-i-minusy-radioupravleniya.html#:~:text=Система%20радиоуправления%20краном%20применяется%20во,преимуществ%2C%20получаемых%20при%20их%20использовании. Плюсы и минусы радиоуправления

АВТОМАТИЗАЦИЯ НА ОСНОВЕ БЕСПИЛОТНОГО АВТОМОБИЛЬНОГО ТРАНСПОРТА

Строкаль Евгений Максимович, студент 2-го курса
Научный руководитель Мельникова Кристина Эдуардовна, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Стремительное развитие автомобильных электронных систем делает реальной идею беспилотного автомобиля. Многие автопроизводители и производители автокомпонентов активно работают над созданием системы автоматического управления автомобилем.

Актуальность исследования обусловлена быстрым развитием робототехники и внедрение ее во всех областях промышленности. Автоматизация на основе робототехники положительно влияет на производительность труда, повышает эффективность производства в целом. Кроме того, позволяет обезопасить человеческий труд исключая человека из опасных производств.

Цель исследования – изучить источники информации и выявить функционал и пользу автономного автомобиля.

Задачи

- изучить алгоритм работы беспилотного автомобиля;
- описать различные виды автономных автомобилей;
- сделать вывод о пользе таких авто.

Объект исследования – беспилотный автомобиль.

Предмет – принцип работы беспилотного автомобиля.

Рассмотрим возможности беспилотного автомобиля. Такой автомобиль имеет возможность выполнять все функции водителя самостоятельно.

К этим функциям относятся:

1) Самостоятельное перемещение в требуемое место, и при этом, автомобиль учитывает все особенности маршрута.

2) Автомобиль способен регулировать скорость самостоятельно. А также способен парковаться самостоятельно.

3) Анализ положения других тс на дороге, а также способность автомобиля беспроблемно перемещаться в условиях недостаточной видимости.

В автоматизации автомобилей присутствует 6 уровней.

На 0-ом уровне автономности машины оборудованы обычным круиз-контролем. Способность регулирования скорости, установленной водителем, не считается автономной технологией.

В 1-ом уровне машины имеют адаптивный круиз-контроль (регулирует и поддерживает скорость транспорта и обеспечивает безопасное расстояние до впереди движущегося автомобиля), вспомогательную систему при парковке и систему оповещения о том, что транспорт сходит с полосы.

Во 2-ом уровне используется помощь в рулевом управлении, в скорости движения автомобиля, и контроль за движением по полосе. Но всё равно водитель обязан держать руки на руле, чтобы при опасных ситуациях взять управление на себя, и предотвратить аварию.

В 3-ем уровне автоматизации транспорт не нуждается в постоянном контроле со стороны человека, т. е. водителю нет необходимости держать руль постоянно. Правда это работает только в идеальных дорожных условиях, и водитель всё равно должен контролировать за ситуацией на дороге, чтобы в случае чего вмешаться в ситуацию и взять управление на себя.

В 4-ом уровне автономности автомобиль может самостоятельно добраться до назначенного места, но только при идеальных дорожных условиях. И если будет начинаться идти дождь или снег, водитель должен взять управление автомобилем на себя.

Разница между 5-ым и 4-ым уровнем в том, что в 5-ом уровне используются 3D-карты местности для того что бы сверятся с ней во время поездки. И если местности не будет на карте, автопилот перейдёт на 3-ий уровень или вовсе отключиться.[1]

Получается 0-ой уровень автономности требует некоторого воздействия человека на автомобиль, а 5-ый уровень может работать самостоятельно. Автомобили пятого уровня уже существуют, но пока что они перевозят только товары.

В качестве примера беспилотного автомобиля давайте рассмотрим модель от Google. Данная модель с помощью датчиков производит сканирование местности. К ним относятся лидары, камеры, радары и высокоточные карты и т.д. Взаимодействие системы такого авто с сервисом Street View, который дает панорамный вид на улицы города.

Лидар – это главный элемент автономного автомобиля. Он устанавливается на крыше авто и представляет собой лазерный дальномер. Лидар генерирует карту в формате 3D в радиусе до 100 метров. Эти данные система объединяет с картами Google, что позволяет ему выбирать оптимальный маршрут и избегать ДТП.

Радар – в машине установлено 4 таких датчика. Этот датчик использует радиоволны для того, чтобы определить расположение объектов и расстояние до них. Излучаемые импульсы отражаются и передаются на антенну. С помощью радара авто способны реагировать на любые изменения.

Датчик положения – этот прибор позволяет определять координаты автомобиля на карте. А с помощью GPS приемника можно определить местоположение автопилота.

Видеокамера установлена возле зеркала заднего вида. Она анализирует сигналы светофоров, а также анализирует ситуацию вокруг. Обычно на автопилотах присутствует около 3 камер. Модель автопилота от Google включает в себя:

- компьютер управления;
- модули датчиков и компьютеры с визуальным интерфейсом;
- рулевое управление с помощью контроллера;
- коммуникационная система;
- система управление с помощью голоса.

Алгоритм работы беспилотного авто выглядит следующим образом:

1) Благодаря лидару формируется карта местности, затем компьютер соединяется с этими данными.

2) После получения информации от датчиков система генерирует алгоритм и начинает оценивать ситуацию на дороге.

3) Компьютер определяет маршрут движения беспилотного авто, а также оценивает поведение других участников.

У автопилота google есть свои особенности. Автономные авто развиваются довольно быстро благодаря тому, что вся собранная информация собирается в общей базе данных и может использоваться всеми автомобилями.

Модели от Google оборудованы возможностью сигналить. Данный сигнал срабатывает при возникновении опасных ситуаций.

В дальнейшем беспилотные автомобили оборудуют возможностью синхронизироваться с ежедневником и календарем. Указав в календаре свои планы, автономная машина сама отвезет человека на деловую встречу или домой в нужное время.

Теперь рассмотрим российский вариант беспилотного автомобиля от Яндекс, который работает примерно по такому же принципу, как и остальные беспилотники. На крыше беспилотника установлены 5 камер, 3 лидара, спутниковой системы навигации GNSS и антенны GPS и мобильной связи GSM, антенна. Спереди у транспорта 4 радара, также to` могут находиться и дополнительные радары. Именно такое сочетание устройств позволяет беспилотнику анализировать информацию вокруг него и строить наиболее безопасную

траекторию движения транспортного средства. Так же ещё используется компьютерное зрение и определённые сенсоры, которые в совокупности помогают контролировать за движением делая его безопасным. С помощью карт высокого разрешения определяется точное местоположение беспилотника и окружающее его местность. И благодаря всем этим устройствам собираются все необходимы данные, и алгоритмом строиться наиболее благоприятный вариант движения автомобиля.[3]

Что бы обрабатывать всю информацию, полученную со всех устройств, в задней части беспилотника находится мощный компьютер, который обрабатывает сотни гигабайтов информации полученной вовремя поездки. Все полученные данные поступают на сервера Яндекс, которые анализируют полученную информацию. Во время движения беспилотник накапливает и анализирует данные, все данные поступают на компьютер, расположенный в задней части машины. Благодаря тому, что автомобиль имеет мощный компьютер с большим объёмом памяти, ему не требуется постоянное подключение к серверу, благодаря чему вовремя поездки автопилоту не требуется быстрый интернет и облачные вычисления, что делает его защищённым от внешних взломов и хакерских атак.[2]

В каждом беспилотнике от Яндекс установлен планшет, что бы люди могли наблюдать за процессом восприятия окружающего беспилотника. Это нужно чтобы люди не волновались и чувствовали себя в безопасности во время поездки. На планшете отображается все показатели, регулирующие и влияющие на движение транспорта. И пока люди ещё не доверяют беспилотному управлению, это отличное решение, что бы пассажир не испытывал сильного беспокойства во время поездки.

Так же в каждом беспилотнике имеется кнопка остановки. Она реагирует на скорость и силу нажатия, т. е. чем быстрее её нажмёшь, тем быстрее автомобиль остановится, или наоборот, чем плавнее нажатие, тем плавнее идёт остановка автомобиля. И обычно такая кнопка находится в руках у водителя-испытателя. Также в машине имеется кнопка перехода в ручной режим управления. Нажав на красную кнопку, включится ручной режим управление, а на зелёную вновь беспилотный режим

Также рассмотрим ещё один вариант зарубежного беспилотного автомобиля под названием Tesla. Его создал всеми не без известный Илон Маск. Что бы не повторяться о принципы работы автономного автомобиля давайте рассмотрим отличительные особенности данной модели. Tesla в отличие от моделей других фирм, для самостоятельного движения не использует лазерные радары. Зато она имеет восемь камер, расположенных на авто, обеспечивающих максимальный угол обзора вокруг беспилотного авто, а также способных видеть объекты на расстоянии до двести пятидесяти метров. Машина так же оборудована двенадцатью ультразвуковыми датчиками, которые дополняют работу камер. Также Tesla использует нейронные сети для анализа информации, которая поступает с датчиков. Эта система называется Tesla Vision. Кроме неё в данной модели присутствует технология Smart Summon. С её помощью можно подать машине сигнал, благодаря которому машина приезжает в то место где находится человек. По сигналу Tesla осуществляет поиск места, где находится источник сигнала. Так же когда вы закончите поездку, автомобиль сам найдёт место и припаркуется. Вызвать машину можно так же и через смартфон.[4]

На сегодняшний день лидерами по разработке автономных авто в России являются компании Яндекс и Cognitive Technologies.

А на мировом рынке лидерами являются: Tesla, Google, Intel MobileEye, Cruise, Ford, Aptiv, UBER, Toyota и другие.

Заключение

В заключение хотелось бы сказать, что вскоре мы окажемся в таком времени где беспилотные авто будут встречаться практически на всех дорогах. Такие автомобили уже признаны в два раза безопаснее транспортных средств под управлением человека, а с учётом того, что каждый раз их будут совершенствовать, беспилотные автомобили смогут полностью заменить водителей.

Список использованных источников

1. Градецкий В.Г., Вешников В.Б., Калиничеко С.В. Управляемое движение мобильных роботов по произвольно ориентированным в пространстве поверхностям. - М.: Наука, 2017

2. Михайлова, Е. А. Беспилотный автомобильный транспорт / Е. А. Михайлова, В. А. Яшенькина. – Текст: непосредственный // Молодой ученый. – 2019. – № 8.2 (246.2). – С. 31-36.

3. Система автоматического управления автомобилем [Электронный ресурс]: http://systemsauto.ru/another/automatic_driving.html

4. Водитель не нужен: шесть уровней автономности машин [Электронный ресурс]: https://trends.rbc.ru/trends/industry

5. Как работает беспилотный автомобиль [Электронный ресурс]: https://bespilot.com/chastye-voprosy/kak-rabotaet-bespilotnyj-avtomobil

ЦИФРОВЫЕ ПРИБОРЫ, ПРИМЕНЯЕМЫЕ В СПОРТЕ

Толмачёв Илья Русланович, студент 2-го курса
Строкаль Евгений Максимович, студент 2-го курса
Научный руководитель Кузьминова Ирина Николаевна, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Цифровые технологии – это новая ступень в развитии человечества. Эти устройства довольно востребованы из-за своего быстродействия и компактности. Данные нововведения не смогли обойти спорт стороной. Эти гаджеты становятся неотъемлемой частью нашей жизни. Они помогают организовать режим дня, здоровое питание, эффективные индивидуальные тренировки и т.д. Нынешняя молодёжь быстро осваивает новые устройства и активно использует их для самосовершенствования.

Гипотеза: изучив источники информации о цифровых устройствах в спорте, мы сможем подобрать комплект устройств для самостоятельных эффективных и удобных физических тренировок.

Цель работы: выбрать цифровые устройства, которые студенты смогут использовать для занятий спортом.

Задачи:

-изучить литературу и интернет-ресурсы по данной теме;

-провести опыт точности измерений цифровых устройств (на примере фитнес браслета).

Актуальность работы: использование современных технологий характерно не только для профессионального спорта, но и для любительского. Современную молодёжь легче увлечь занятием спортом с помощью цифровых устройств.

Современные устройства, используемые в спорте, неплохо подходят для сохранения хорошей физической формы, а также превращают спортивные тренировки в увлекательное и полезное занятие. Также с помощью устройств можно отслеживать множество показателей. К этим показателям относятся: сожжённые калории, пройденное расстояние и т.д.

Такие приборы популярны в спорте, так как они очень удобны в использовании. Так, например, интеллектуальное оборудование (высокотехнологичные шлемы, футболки, кроссовки или накладки т.д.) позволяет выполнять регулярные анализы игрока на предмет безопасности и травм. А социальные медиа и цифровые платформы для спорта позволяют лучше освещать спортивные события, а также позволяют пользователям договариваться о совместных тренировках и марафонах в режимах онлайн и офлайн. Таких девайсов, предназначенных для спорта, существует огромное количество.

Рассмотрим принцип работы нескольких приборов и выберем для себя наиболее подходящие.

Мини-компьютер в очках

Рассмотрим данное устройство на примере «ReconJet». В «ReconJet» интегрирован мощный компьютер на базе 2-ядерного процессора ARM Cortex-A9 с тактовой частотой 1,2 ГГц. Всё это позволяет собирать нужную информацию и анализировать её, повышая качество итоговых показателей. Данные очки созданы для занятий спортом вне дома или зала. Управление осуществляется с помощью датчиков, находящихся сбоку, на сенсорной панели. Программное обеспечение этого гаджета подходит только для 3 видов деятельности, – триатлона, бега и велоспорта, – в будущем их будет больше. Стоимость этого девайса составляет около 30000 рублей. За эту цену мы получим устройство с большим функционалом:

- определение текущего местоположения с помощью навигатора;

- запись, воспроизведение, изменение масштаба изображения, контроль за снимаемым изображением с помощью видеокамеры;
- распознавание речи с помощью микрофона;
- датчик температуры;
- 8 ГБ памяти;
- программа «цифровой помощник»;
- возможность подключения к телефону.

Преимущества очков:

- многофункциональность, компактность.

Недостатки:

- большая цена.

Кроссовки для бега

Это не обычные кроссовки, а специально разработанная обувь с датчиками. Речь идет о датчиках «AdidasmiCoachSpeedCell», которые вставляются в подошву бутс и считывают различные показания, необходимые для отслеживания результативности спортсмена, и передают их на смартфон. Также датчики помогают отследить и исправить основные ошибки в технике бега. Помимо этого, кроссовки способны подсказывать основные рекомендации для бега.

Преимущества кроссовок:

- сбор и анализ информации о техники бега.
- большой функционал, простейшее в использовании приложение.

Недостатки:

- нельзя подключиться к GPS, долгий процесс синхронизации.
- небольшой по объёму заряда аккумулятор.
- не высокая цена.

Потенциал таких кроссовок очень большой. С ними футбольные тренировки будут проходить намного эффективнее, а также появится возможность для каждого человека заниматься спортом самостоятельно, регулярно отслеживая свои скоростные показатели.

Монитор сердечного ритма

Данное устройство позволяет отслеживать ритм человеческого сердца. Его надевают на грудную клетку, и с помощью импульсов он считывает сердцебиение. Это устройство будет весьма полезно на тренировках, потому что благодаря нему можно поддерживать пульс на определённом уровне, что делает такие тренировки весьма эффективными.

Достоинства:

- контроль частоты сердечных сокращений, поддержания пульса в нужной зоне.
- совместимость со смартфоном.
- более точное списывание показания, нежели у других подобных устройств.
- возможность заниматься спортом даже при заболеваниях сердца.

Недостатки:

- дискомфорт при ношении.
- неэффективность использования в интервальных видах тренировок.
- необходимы специальные знания о зонах работы сердца.
- цена на это устройство составляет около 5000 рублей.

Этот гаджет нельзя будет использовать при активных и динамических тренировках. Мы считаем, что это устройство нам не подойдёт, но зато подойдёт для тех людей, у которых есть проблемы с сердцем.

Умные гантели

Это устройство предназначено для людей, которые предпочитают силовые нагрузки гантелями. Данные гантели могут подсчитывать за вас сделанные упражнения. Также они

имеют динамик, который будет издавать определённый звук при достижении поставленной задачи в тренировке.

Плюсы данного гаджета:

- отличный хват, удобная конструкция.
- обладает приложением с большим спектром функций.

Минусы:

- плохая синхронизация.
- нагрузочная способность имеет предел.

Ценник за один комплект начинается от 2400 рублей.

Примером такого гаджета являются гантели C-RingDumbbells. Они обладают уникальным дизайном и подсветкой. Устройство предназначено для выполнения упражнений с отягощением мышц. После подсчитывания сожженных калорий гаджет извещает человека о результатах с помощью подсветки 3 цветов. С помощью этого человек может отслеживать свои результаты и планировать дальнейшие тренировки. Эти результаты можно отслеживать на смартфоне, подключив к нему гантели через Wi-Fi или Bluetooth.

Тренировочная маска

Эту маску используют для повышения выносливости. Данный гаджет работает по принципу ограничения поступления кислорода к человеку во время тренировки. Такие упражнения положительно влияют на выносливость организма.

Устройство представляет из себя маску с клапанами для вдоха и выдоха с регулируемым сопротивлением. Она способствует правильному дыханию во время физических упражнений.

Достоинства тренировочной маски:

- прокачка мышц дыхательной системы.
- сосредоточение на дыхании во время тренировок.
- эффективное использование кислорода во время тренировок.
- многообразие тренировок, уникальный дизайн.

Недостатки:

- есть некоторые ограничения в использовании, большой размер.

Примером такой тренировочной маски служит Elevation. В данном приспособлении используют многоступенчатую систему клапанов для регулирования поступления воздуха. После нескольких упражнений с использованием этой маски объём лёгких увеличится.

Цены тренировочных масок составляет около 1800-7000 рублей.

Фитнес-браслет

Этот девайс создали с целью отслеживания показателей человека в любой момент времени. Определение показателей осуществляется с помощью датчиков. Примером таких датчиков является акселерометр, который реагирует на перемещение тела в пространстве, и гироскоп, использующийся для определения положение человека в пространстве.

Но самыми важными, по нашему мнению, являются датчики измерения пульса, давления. Пульс определяет датчик со светодиодами, работа которого основана на свойствах кровотока меняться в разные периоды сердечных пульсаций и по-разному отражать свет. Определение давления происходит на основе частоты и скорости пульсаций, человеческого тела. Для удобства можно подключить свой смартфон к фитнес-браслету через Bluetooth, чтобы отслеживать в нём нужные вам параметры (количество пройденных шагов, сожженных калорий и т.д.).

Достоинства устройства:

- считывание количества пройденных шагов и расстояний.
- умное пробуждение.
- измерение пульса, давления.
- аккумулятор с большой ёмкостью, удобство использования.

Недостатки устройства:

- в некоторых моделях нет дисплея.
- отсутствие водонепроницаемости, относительно малый срок службы.

Эти "Спортивные часы" обрели огромную популярность среди людей, любящих спорт. Это неудивительно, потому что за небольшую стоимость вы получаете большой спектр функций. Цена такого устройства начинается от 800 рублей.

Эксперимент с фитнес-браслетом

Проведём небольшой эксперимент с фитнес-браслетом. Сравним точность измерения часов с тонометром. В течение трёх дней будем измерять давление и пульс с помощью фитнес-браслета, сравнивая показания с тонометром. Результаты измерений будем записывать в таблицу.

	Показания фитнес-браслета	**Показания тонометра**	**Разница показаний**
Пульс (первый день)	70	69	1
Давление (первый день)	118/72	116/69	2/3
Пульс (второй день)	64	62	2
Давление (второй день)	145/69	144/72	1/3
Пульс (третий день)	68	68	0
Давление (третий день)	101/70	102/72	1/2

В результате эксперимента мы выяснили, что фитнес-браслет способен довольно точно определять биологические показатели человека, если не брать в расчет небольшие погрешности. За относительно невысокую стоимость это очень полезный девайс, особенно для спортсменов.

В итоге мы пришли к следующим выводам:

1. Существует огромное количество цифровых устройства для спорта, как полезных, так и не совсем.

2. Среди всего многообразия цифровых устройств для спорта самыми подходящими для студентов мы считаем фитнес-браслет и умные кроссовки для бега, так как они стоят относительно недорого и обладают многими функциями, которые сделают тренировку намного удобней и продуктивней.

Сегодня цифровые технологии всё больше входят в нашу жизнь и в спорт. Благодаря таким технологиям появляется возможность отслеживания практически всех физических показателей, что позволяет сделать процесс тренировки более безопасным и интересным. Но самое главное, данные гаджеты вовлекают в здоровый образ жизни всё большее количество людей.

Список использованных источников

1. [Электронный носитель] https://technosova.ru/cifrovaja-tehnika/gadzhety/top-10-sportivnyh-gadzhetov/
2. [Электронный носитель] https://topfitnesbraslet.ru/blog/kak-rabotaet-fitnes-braslet
3. [Электронный носитель] https://my-soccer.ru/obzory/futbolnye-trenirovki-s-datchikom-adidas-micoach-speed-cell/
4. [Электронный носитель] https://gadgetpage.ru/gadzhety/2279-ustrojstvo-funkcii-harakteristiki-i-preimuschestva-fitnes-brasletov.html
5. Тимошенков В.В. и др. Основные направления применения вычислительной техники в физической культуре и спорте //Теор. и практ. физ. культ. 1993, №1
6. Фатеенков М. М., Чернышева И. В., Егорычева Е. В., Шлемова М. В., Мустафина Д. А. СОВРЕМЕННЫЕ ТЕХНОЛОГИИ В СПОРТЕ // Международный студенческий научный вестник. — 2015. — № 5–4.

РАЗРАБОТКА И МОДЕЛИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПОВЕРКИ ГАЗОАНАЛИЗАТОРОВ, СТАРООСКОЛЬСКИЙ ОТДЕЛ ФБУ «БЕЛГОРОДСКИЙ ЦСМ»

Цапков Алексей Иванович, студент 4-го курса
Научный руководитель Мельникова Кристина Эдуардовна, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Использование программного обеспечения для управления процессом поверки и калибровки обеспечивает учет средств измерений, хранение результатов поверки и калибровки всех средств измерений, когда-либо находящихся в данной метрологической службе, отслеживаниесредств измерений, у которых истек или истекает межповерочный интервал, а также позволяет проводить анализ информации по средствам поверки.

Актуальность исследования заключается в сокращении времени на поверку газосигнализаторов и объема затрат на расходный материал, а также в обеспечении удаленного управления системой, за счет установки генератора газовых смесей для точной и быстрой регулировки расхода и концентрации, а также персонального компьютера, что позволит обеспечить бесконтактный метод поверки и, следовательно, обезопасить работу персонала.

Целью исследования является автоматизация системы регулирования расхода и концентрации газа на метрологическом стенде для поверки и калибровки газоанализаторов.

Задачи исследования:

- описать существующий уровень автоматизации на метрологическом стенде для поверки газоанализаторов;
- выявить недостатки существующей системы автоматизации;
- определить задачи модернизации;
- выбрать техническое и программное обеспечение, дать его обоснование.

Объект исследования - метрологический стенд для поверки газоанализаторов ФБУ «Белгородский ЦСМ» Старооскольский отдел.

Предмет исследования - автоматизированная система управления метрологического стенда для поверки газоанализаторов.

Федеральное бюджетное учреждение «Государственный региональный центр стандартизации, метрологии и испытаний в Белгородской области» осуществляет работы по обеспечению единства измерений на территории Белгородской области.

Процесс поверки газоанализатора осуществляется при помощи метрологического стенда для поверки и калибровки газоанализаторов и газосигнализаторов.

Принцип работы метрологического стенда заключается в том, что из баллона, находящегося под избыточным давлением через трубку подается газ на газоанализатор. Необходимый расход задается при помощи редуктора с вентилем точной регулировки, опираясь на показания ротаметра. При помощи комбинированного электроизмерительного прибора снимаются показания с поверяемого прибора и рассчитывается погрешность показаний.[2]

Поверка газоанализатора с помощью метрологического стенда производится несколькими этапами: определение необходимого баллона с подходящей концентрацией; присоединение баллона к метрологическому стенду при помощи трубок; регулирование расхода газа; снятие показаний; расчет погрешности.[1]

Уровень автоматизации метрологического стенда для поверки газоанализаторов крайне низкий.Перед поверкой прибора определяется подходящий по концентрации баллон с газом и производится герметичное подключение его к метрологическому стенду.

Первым недостатком системы автоматизации стенда является ручная регулировка расхода газа, что влечет за собой неточности измерений.

Вторым недостатком существующего метрологического стенда является непосредственное участие человека в процессе поверки. Существующий метрологический стенд оборудован вытяжной вентиляцией, но она не обеспечивает полную безопасность от газа, используемого в процессе поверки.

Третьим существенным недостатком является потребность в приобретении большого количества баллонов с газовыми смесями, так как для каждого определенного типа газоанализаторов необходимо присоединять баллон с определенной концентрацией газа. Данный процесс занимает большой объем времени, физических усилий, а также материальных затрат на приобретение.[5]

Для упрощения поверки газоанализаторов и сокращения времени на поверку предлагается выполнить следующие задачи:

1. Осуществление автоматической регулировки расход газа, а также автоматизации создания необходимой концентрации газовой смеси;
2. Обеспечение автоматического удаленного оперативного управления генератором;
3. Осуществление безопасного использования в работе газовых смесей с любыми компонентами.

Для реализации поставленныхзадач предлагается подключить и заменить следующие устройства:

1) Генератор газовых смесей ГГС-03-03. Он предоставляет возможность автоматически регулировать расход газа, а также создавать необходимую концентрацию газовой смеси, путем смешения необходимого газа высокой концентрации с газом разбавителем, что позволяет исключить потребность в приобретении большого количества баллонов с исходными газовыми смесями различных концентраций. Так как работа по приготовлению смесей данного генератора очень точна, соответственно, точность измерений при поверке увеличится, а затраты времени на подключение различных баллонов и ресурсов значительно уменьшатся.[3]

2) Станция оператора с персональным компьютеромпредназначена для автоматического удаленного оперативного управления генератором. Благодаря интуитивно понятному интерфейсу программного обеспечения сокращается время на задание по смешению газовой смеси определенной концентрации и время на регулировку расхода.

3) Лабораторный вытяжной шкаф ШВДГн-311 для поверки и калибровки газоанализаторов, представляет собой цельнометаллическую конструкцию. Конструкция шкафов обеспечивает изолированную рабочую зону с организованной вытяжной вентиляцией. Это дает возможность безопасно использовать в работе газовые смеси с любыми компонентами. Шкафы ШВДГн-311 позволяют решать широкий спектр газоаналитических задач, при этом экономит рабочее пространство и оптимизирует работу сотрудников.

4) Выбор программного обеспечения. Программа управления генератором газовых смесей ГГС-03-03.Программное обеспечение генераторов состоит из двух модулей - встроенного и автономного.Автономное программное обеспечение генераторов для персонального компьютера под управлением ОС семейства Windows предназначено для задания режимов работы генераторов и просмотров результатов измерений в реальном времени. Программное обеспечение является полностью метрологическизначимым.Программа обладает удобным русскоязычным интерфейсом, что позволяет быстро и качественно управлять генератором.[4]

Таким образом, автоматизация системы регулирования расхода и концентрации газа на метрологическом стенде для поверки и калибровки газоанализаторов позволит:

- автоматизировать регулировку расхода газа;
- обезопасить работу персонала;
- экономить ресурсы и затраты на приобретение баллонов с ГС;

- экономить затрачиваемое время на поверку;
- повысить точность поверки.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Микрюков В.Ю. Безопасность жизнедеятельности: учебник / В.Ю. Микрюков. - 10-е изд., перераб. и доп. – Москва : КНОРУС, 2019. – 282 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Суркова Л. Е. Моделирование систем автоматизации и управления технологическими процессами: практикум / Л. Е. Суркова, Н. В. Мокрова. — Саратов : Вузовское образование, 2019. — 46 c. — ISBN 978-5-4487-0496-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/82692.html. — Режим доступа: для авторизир. пользователей

5. Termexlab [Электронный ресурс]: https://termexlab.ru/ru/product/shvdgn

ПРОГРАММИРОВАНИЕ НА ЯЗЫКЕ FBDB СРЕДЕ ONIPLRДЛЯ ПРОИЗВОДСТВА

Царегородцев Лев Евгеньевич, студент 2 курса
Научный руководитель Комарова Юлия Викторовна, преподаватель 1 категории
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Любой технологический процесс современного производства полностью или частично автоматизирован. Промышленная автоматика уже более 50 лет не обходиться без программируемых логических контроллеров (ПЛК).

ПЛК – это электронное специализированное устройство, выполняющее функции управленияпоследовательнымипроцессами,в соответствии с заложенным алгоритмом, с использованием информации, получаемой от датчиков для определения состояния объекта и выдачи управляющих воздействий.

Применение ПЛК в системе автоматизации позволяет:

1. сократить этап разработки,
2. упростить процесс монтажа и отладки за счет стандартизации отдельных аппаратных и программных компонентов,
3. обеспечить повышенную надежность в процессе эксплуатации,
4. предусмотреть удобный ремонт и модернизацию при необходимости.

Система программирования – это одна из полезных особенностей ПЛК.Программированиеупрощает разработку управляющей программы для специалистов различного профиля. Программирование в ПЛК производиться с помощью составления на экране компьютера визуальных цепей из релейных контактов для описания операторов программы. Подобное программирование называют языком релейной логики. [4]

В настоящее время существуют пять языков, стандартизованных для всех платформ ПЛК. Три графических и два текстовых языка программирования взаимно совместимы. При этом одна часть программы может создаваться на одном языке, а другая — на другом, более удобном для нее.

К графическим средствам программирования ПЛК относятся язык последовательных функциональных блоков (SequentialFunctionChart, SFC), язык релейных диаграмм (LadderDiagram, LD) и язык функциональных блоковых диаграмм (FunctionBlockDiagram, FBD), используемый при сдаче Демонстрационного Экзамена по стандартам WorldSkills. Для программистов более привычными являются язык структурированного текста (StatementList, STL), напоминающий Паскаль, и язык инструкций (InstructionList, IL), похожий на типичный Ассемблер.

В России первое место по популярности занимает язык STL,второе место по популярности занимает графический язык FBD, далее следует язык LD

FBD является графическим языком и наиболее удобен для программирования процессов прохождения сигналов через функциональные блоки. Язык FBD пользователей, которые легко могут составить электрическую схему системы управления на "жесткой логике", но не имеют опыта программирования.[1]

Написанная на данном языке программа для контроллера представляет собой набор связанных друг с другом функциональных блоков, выходы и входы которых соединены линиями соединений. Линии соединений отражают определенные программные переменные, через которые происходит обмен данными от блока — к блоку.

Отдельный блок несет на себе конкретную функцию: «И», «ИЛИ», «НЕ», счетчик.Каждый блок может иметь несколько выходов и входов. Из таких блоков графически составляются выражения, образующие цепи: к выходу одного блока присоединяется следующий блок, далее — еще блок, и так образуются цепи. По ходу цепи

порядок выполнения блоков соответствует порядку их соединения, а результат выполнения цепи либо подается на выход ПЛК, либо записывается в какую-то внутреннюю переменную.[2]

На рисунке 1 приведен пример фрагмента программы на языке функциональных блоковых диаграмм FBD: A поделить на B , умножить на 2 и записать в переменную result.

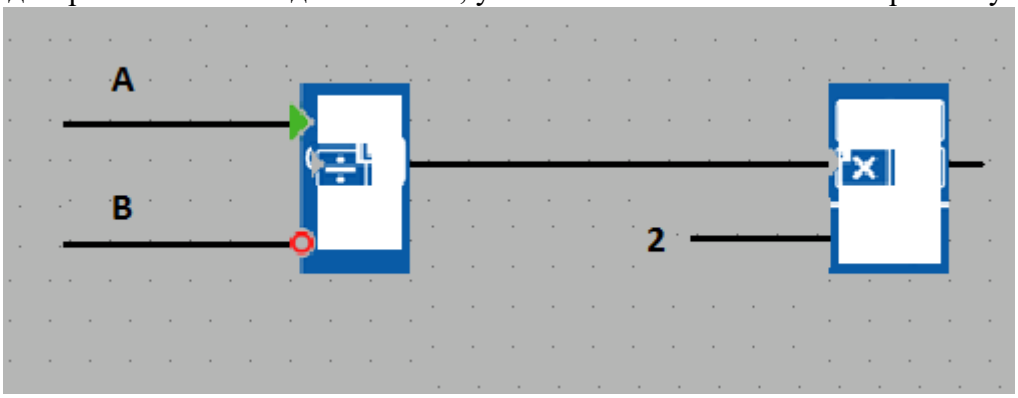


Рисунок 1 - Пример фрагмента программы на языке FBD

Одним из крупнейших российских производителей ПЛК является компания IEK GROUP. Вся продукция промышленной автоматики объединена торговой маркой ONI.

Программирование ПЛК производится в программной среде ONIPLR. Бесплатное свободно распространяемое программное обеспечение ONI PLR Studioc интуитивно понятным нтерфейсом и языком функциональных блоковых диаграмм.

Программируемое логическое реле ONI PLR-Sявляется оборудованием класса микро и наноПЛК. Оно предназначено для построения систем автоматизированного управления технологических процессов работы на: тепличных комплексах, насосных станциях, котельных, конвейерах, приточно-вытяжной и промышленной вентиляциях, дозаторах, системах сбора и возврата конденсата, системах водоснабжения, водоотведенияи водоподготовки, системах электроснабжения и освещения.[3]

На любом производстве есть электродвигатель, который необходимо запустить, остановить, а по требованиям технологии осуществить реверс. На рисунке 2 представлена схема запуска, реверса и остановки электродвигателя, а на рисунке 3 программа на языке FBD в среде ONIPLR.

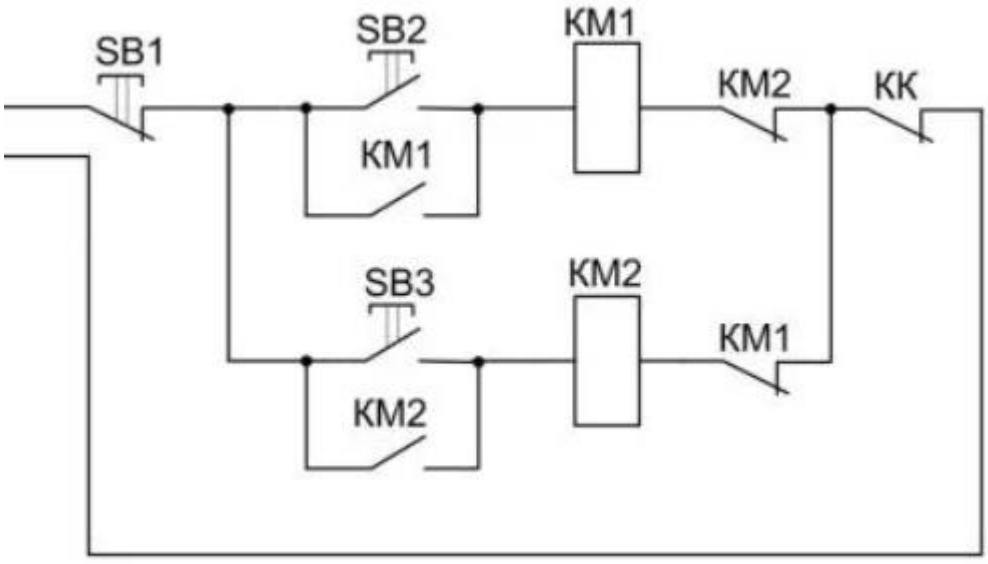


Рисунок 2 – Контакторная схема запуска реверсивного двигателя

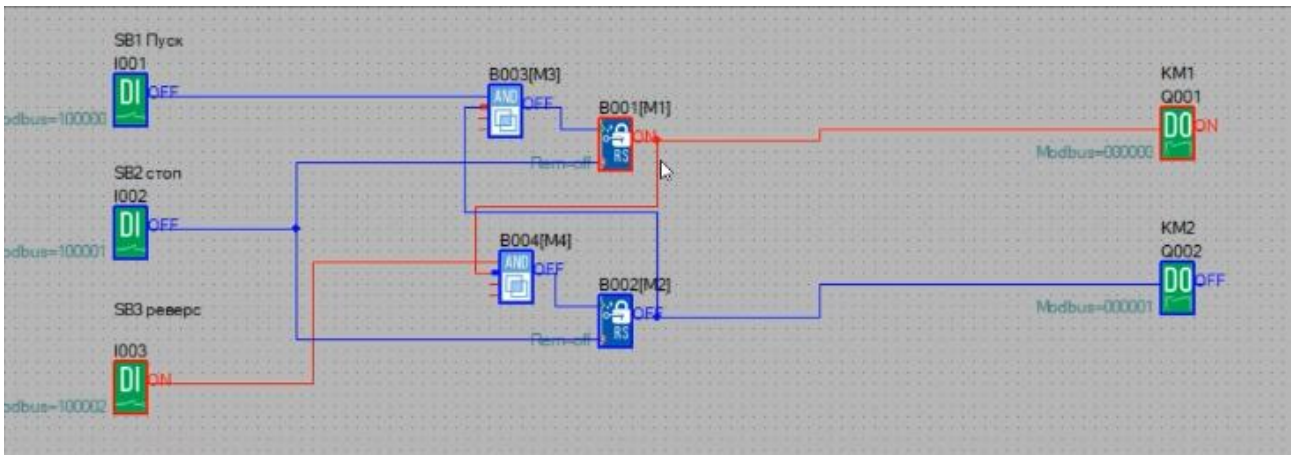


Рисунок 3 – Программа для ПЛК на языке FBD в среде ONIPLR

Список использованных источников

1.bookASUTP.ru«Системы программирования на языках МЭК 61131-3» [Электронный ресурс]. URL: https://bookasutp.ru/Chapter9_3.aspx.

2. ELEKTRIKINFO«Язык функциональных блоковых диаграмм (FBD) и его применение»[Электронный ресурс].URL:http://electrik.info/main/automation/1320-yazyk-funkcionalnyh-blokovyh-diagramm-fbd-i-ego-primenenie.html.

3. PLR-S СИСТЕМНОЕ РУКОВОДСТВО[Электронный ресурс]. URL:http://oni-system.ru/upload/oni-system/produktsiya.

4. Компэл «Введение в ПЛК: что такое программируемый логический контроллер» [Электронный ресурс]. URL: https://www.compel.ru/lib/95591.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ НАСОСНОЙ СТАНЦИИ ОБОРОТНОГО ВОДОСНАБЖЕНИЯ ВТОРОГО ПОДЪЕМА ДЛЯ ПОДАЧИ ВОДЫ НА ОФ АО «ЛГОК»

Юрченко Иван Владимирович, студент 4-го курса
Научный руководитель Мельникова Кристина Эдуардовна, преподаватель
Оскольский политехнический колледж
Старооскольский технологический институт им. А.А. УГАРОВА (филиал)
федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»,
город Старый Оскол

Стратегически важным направлением развития промышленности является повышение качества и увеличение скорости прохождения технологических процессов на предприятиях путем автоматизации этих процессов. Сейчас невозможно представить какой-либо сложный технологический процесс, выполняемый без участия систем автоматизации, без применения новейших разработок, в сфере электронно-вычислительной техники и программного обеспечения, существование современного предприятия представляется невозможной. Автоматизированные системы управления призваны обеспечить существенное увеличение производительности труда, улучшение качества выпускаемой продукции и других технико-экономических показателей закачки перекачки технической воды [1].

Целью исследования является расширенный анализ автоматизированной системы управления насосной станции оборотного водоснабжения второго подъема для подачи воды на ОФ АО «ЛГОК».

Задачи исследования:

– изучить характеристику технологического процесса насосной станции оборотного водоснабжения второго подъема;

– проанализировать существующий уровень автоматизации;

– выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является насосной станции оборотного водоснабжения второго подъема для подачи воды на ОФ АО «ЛГОК».

Предмет исследования автоматизированная система управления насосной станции оборотного водоснабжения второго подъема для подачи воды на ОФ АО «ЛГОК».

Насосная станция оборотного водоснабжения второго подъема предназначена для подачи воды на обогатительную фабрику и поддержания давления в трубах, в зависимости от качества руды.

В насосной станции оборотного водоснабжения второго подъема установлено семь насосных агрегатов. Для повышения эксплуатационной надежности насосной станции в торцевой стене машинного зала заложена труба аварийного сброса. Насосы предназначены для перекачивания воды и жидкостей, имеющих сходные с водой свойства.

Существующая система автоматического управления насосной станцией является частью системы автоматизации обогащения железной руды и осветления жидкой фазы пульпы. Управление технологическим процессом, пуск оборудования и контроль за его работой осуществляется централизованно операторами с пультов управления.

Насосная станция оборотного водоснабжения второго подъема оснащена системой автоматического контроля и регулирования давления воды в трубах, состоящей из датчика плотности и расходомера - счетчика. Сигналы, поступающие с датчиков, поступают на регулятор, который обрабатывает и выдает полученные значения оператору. В соответствии с полученными значениями оператор открывая или закрывая напорные задвижки, либо запуская или останавливая насосы производит регулировку давления – метод дросселирования. Это один из наиболее распространенных методов изменения

характеристики сети. Однако этот метод снижает КПД насосной установки за счет разности между напором, развиваемым насосом, и напором, требуемым в сети [2].

В ходе анализа существующего уровня автоматизации выявлены следующие недостатки:

– используемое оборудование морально и физически устарело;

– недостаточная надёжность работы оборудования;

– низкое качество управления, т.к. управление подачей воды производится вручную машинистом насосной станции;

– регулирование давлением в водоводах осуществляется в ручном режиме.

Для устранения указанных недостатков предлагается:

1) заменить морально устаревший контроллер;
2) внедрить частотно-регулируемый электропривод для насосов;
3) модернизировать систему визуализации;
4) стабилизировать давление в общем коллекторе.

Для решения поставленных задача выбрано следующее оборудование:

1. Преобразователи частоты ВЧРП т.к. он разработан с учетом требований отечественных стандартов, полностью адаптирован к эксплуатации в российских условиях, имеет интуитивно понятный интерфейс на русском языке.

2. Частотный преобразователь ROBICON Perfect Harmony. Применение преобразователя частоты Perfect Harmony позволяет добиться значения коэффициента мощности cos φ более 0,95 без применения дополнительных устройств компенсации реактивной мощности. А также он поддерживает каскадный запуск двигателей, при котором двигатели поочерёдно пускаются в режиме плавного пуска и передаются на сеть. Последний запущенный двигатель может быть оставлен в регулируемом режиме для обеспечения точного расхода.

3. В качестве датчика температуры выбираем термометр сопротивления медный ТС 014-50М.В3. Термопреобразователи сопротивления с кабельным выводом предназначены для измерения температуры различных рабочих сред (вода, газ, пар, другие химические соединения, сыпучие материалы) и могут быть использованы во всех отраслях промышленности.

4. В качестве датчика положения выбираем ПКП1И-Н. Обеспечивает контроль положения задвижки по числу оборотов вала с помощью датчика импульсов.

5. Выбираем программируемый контроллер SIMATIC S7-1500 с CPU 1513-1 PN, для построения систем управления, требующих выполнения программ среднего объема, средней/ высокой скорости обработки данных и обслуживания систем распределенного ввода-вывода на основе сети PROFINET IO.

6. Для SIMATIC S7-1500 будет разработано программное обеспечение. Программирование контроллера осуществляется на специальном языке STEP 7 Professional V12.

SIMATIC STEP 7 Professional V12 - это система проектирования для программируемых контроллеров SIMATIC серий S7-1200, S7-300, S7-400, WinAC. Обеспечивает оптимальную поддержку новых программируемых контроллеров серии SIMATIC S7-1500 [8].

STEP 7 V12 базируется на функциональных возможностях единой рабочей среды проектирования Totally Integrated Automation Portal (TIA Portal), которая позволяет выполнять однородную, эффективную и интуитивно понятную разработку решений для всех задач автоматизации.

Модернизация позволит:

– повысить безопасность и надежность работы насосной станции, уменьшить вероятности возникновения аварийных ситуаций за счет автоматизации контроля и управления оборудованием;

– сократить время восстановления работы насосной станции в аварийных ситуациях;

– сократить потери электроэнергии насосной станции за счет оптимизации режима работы насосов;

– улучить информированность обслуживающего персонала;

– улучшить условия труда персонала.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. — 2-е изд. — Саратов : Ай Пи Эр Медиа, 2019. — 459 с. — ISBN 978-5-4486-0574-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83341.html. — Режим доступа: для авторизир. пользователей

5. АО «ЛГОК» [Электронный ресурс]: https://www.metalloinvest. com/business/mining-segment/lgok/. Официальный сайт.

6.Siemens [Электронный ресурс]: https://new.siemens.com/ru/ru/produkty/avtomatizacia/sistemy-avtomatizacii/promyshlennye-sistemysimatic/kontroller-simatic/simatic-s7-1500.html - Simatic S7-1500. Официальный сайт.

Секция 2.2

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ТЯГОВОЙ ПОДСТАНЦИИ ООО «СКОРОСТНОЙ ТРАМВАЙ»

Балабуркин Михаил Васильевич, студент 4-го курса
Научный руководитель Азарова Виктория Сергеевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Тяговая подстанция трамвая - предназначена для передачи электроэнергии от ЛЭП в контактную сеть трамвая.

На подстанции осуществляется преобразование трёхфазного переменного тока в выпрямленный постоянный. Первые тяговые подстанции трамвая были оборудованы одноякорными электромашинными преобразователями тока - умформерами, позднее стали применяться ртутные выпрямители тока.

КПД умформера в номинальном режиме работы составлял 88-89 %, КПД ртутного выпрямителя не превышал 94,5 %. Эксплуатация ртутных выпрямителей была сложной и требовала соблюдения персоналом предосторожностей при работе со ртутью. С 1965 года на тяговых подстанциях трамвая используются полупроводниковые преобразователи на диодах или тиристорах, обеспечивающие высокую надёжность и экологическую чистоту процесса преобразования тока; КПД их достигает 97,5 % [2].

Целью исследования является расширенный анализ АСУ тяговой подстанции ООО «Скоростной трамвай».

Задачи исследования:

– предоставить общие сведения о ООО «Скоростной трамвай» и краткую характеристику технологического процесса;

– описать технологические параметры тяговой подстанции;

– проанализировать существующий уровень автоматизации;

– выявить недостатки существующей системы управления и определить задачи для модернизации системы управления;

– разработать математическую модель системы управления и построить графики переходных процессов;

– выбрать и обосновать техническое и программное обеспечение;

– рассмотреть вопросы охраны труда и организационно-технические мероприятия по пожарной безопасности.

Объектом исследования является тяговая подстанция ООО «Скоростной трамвай».

Предметом исследования является автоматизированная система управления тяговой подстанцией ООО «Скоростной трамвай».

Объектом автоматизации является тяговая подстанция установленная за городом ООО «Скоростной трамвай». Тяговая подстанция - электроустановка, предназначенная для понижения электрического напряжения и последующего преобразования (выпрямления) тока (для подстанций постоянного тока) с целью передачи его в контактную сеть для обеспечения электрической энергией трамваев [1].

Схема РУ-10 кВ тяговой подстанции собрана из двух секций шин. Ввод электроэнергии осуществляется кабелями: секция №1 получает питание от одной кабельной линии, секция №2 - от второй кабельной линии, проведенных от районной подстанции. Для совместной работы шин предусмотрен секционный выключатель, оборудованный устройствами защиты.

Распределительное устройство 10 кВ со сборными алюминиевыми шинами размещают в здании подстанции. РУ-10 кВ монтируют из комплектных камер внутренней

установки К-99, которые собираются в ряд по шкафам. Шкафы оборудованы выкатными выключателями. ЗРУ-10кВ расчитано на десять камер позволяющих обеспечить питание двух преобразователей, двух ТСН, двух ТН, трех отходящих фидеров и понижающий трансформатор для питания фидеров ПЭ. В состав ЗРУ также входят хозяйственная камера и камера секционного выключателя и ОПН. В здании подстанции также находится РУ-6 кВ СЦБ. Отходящие фидера РУ-10 кВ сделаны кабельными. Чтобы можно было определить фидер, на котором произошло однофазное КЗ, кабельные линии снабжены трансформаторами тока нулевой последовательности (фидера №1 и №2 поста ЭЦ). Контроль напряжения на секциях шин РУ-10 кВ, а также питание приборов учета энергии и устройства контроля изоляции фаз системы 10 кВ осуществляется с помощью ТН, для которых используются камеры, включающие в себя ТН подключенный к сборным шинам через предохранитель и разъединитель с заземляющими ножами. Параллельно ТН подключен нелинейный ограничитель напряжения.

От каждой секции сборных шин получают питание тяговый трансформатор типа ТРДП 12500/10 ЖУ 1. От тягового трансформатора пониженное напряжение подается по алюминиевым шинам на выпрямительный агрегат типа ТПДЕЖ - 3,15к - 3,3к УХЛ 4 с 12пульсной системой выпрямления внутренней установки. Установка тяговых трансформаторов предусмотрена на открытой части тяговой подстанции между подъездным ж/д путем и зданием подстанции. Кремневый выпрямитель расположен внутри здания подстанции, где расположено РУ-3,3 кВ. подстанция реконструкция заземление молниезащита

Электрическая связь РУ-10 кВ - тяговый трансформатор осуществляется с помощью кабелей, проложенных в кабельных колодцах. Электрические связи: тяговый трансформатор - проходная плита - кремневый выпрямитель.

1 Запуск и выполнение программы;

1.1. Включить сетевой фильтр и источник бесперебойного питания вставить электронный ключ защиты в разъем системного блока.;

1.2. Включить системный блок, т.е., нажать на сетевой выключатель - клавишу; «0». Программа начнет загружаться автоматически или загрузить из меню «ПУСКА СТМ «Скоростной трамвай» Базовое ПО Менеджер задач СО СА-Сервер. После загрузки на экране видеомонитора АРМ оператора появится мнемосхема КП1 (7П-1). Мнемосхема содержит полную информацию текущем состоянии контролируемых объектов. Любую мнемосхему можно вызвать с помощью кнопок перехода, расположенных в нижней части мнемосхемы, то есть, при нажатии левой клавишей мыши на кнопку нужного КИ, на экране выдается мнемосхема с контролируемыми параметрами этого КП

В центре управления тяговыми подстанциями применяются:

1) Измерительный преобразователь постоянного тока ФЕ1875-АД предназначен для преобразования электрических сигналов постоянного тока, постоянного напряжения, сигналов от стандартных термопреобразователей сопротивления (ТС) и термопар в унифицированные сигналы постоянного тока или напряжения с возможностью выдачи измерительных данных в цифровом виде и передачи их по стандартному интерфейсу.

2) Интеллектуальные панели управления Power Panel PP41 являются результатом объединения панели оператора и контроллера в едином устройстве, обеспечивающем эффективное выполнение задач управления и визуализации.

3) Программирование панелей управления Power Panel осуществляется с использованием единого инструментального программного обеспечения - B&R Automation StudioTM. Функции управления в реальном времени гибко сочетаются с интерфейсом оператора в виде символьного или графического дисплея.

4) Внедрение терминалов микропроцессорных защит и автоматики в систему управления электроснабжением ЭТ способствует достижению следующих целей:

1. Повышение контроля за своевременностью и качеством устранения повреждений технических устройств электроснабжения;

2. Систематизация данных по выявленным отказам технических устройств для анализа состояния безопасности движения поездов;

3. Снижение трудоемкости работ при формировании отчетно - учетной документации, повышение скорости обработки и передачи документации между всеми уровнями управления.

Трамвай может рекуперировать энергию. Но практически вся рекуперированная энергия электрифицированного транспорта «сжигается» на тормозных резисторах и повторно не используется. Резкие изменения напряжения в сети. Недостаток сетевой мощности на отдельных участках движения.

Режим быстрого запасания рекуперированной электроподвижным составом энергии с последующей быстрой отдачей, для применения на городском электрифицированном транспорте. Сглаживание колебаний напряжения в сети. Работа в качестве параллельного генератора

Недостатком трамвая является малое использование рекуперированной энергии.

Трамвай может возвращать энергию. Но почти вся рекуперированная энергия электрифицированного транспорта «сжигается» на тормозных резисторах и повторно не используется. Резкие изменения напряжения в сети. Так же существует недостаток сетевой мощности на отдельных участках движения.

Для модернизации АСУ предлагается:

Общая постановка цели, это установка нового оборудования с минимизацией объема процедур технического обслуживания, увеличением срока службы, а значит и увеличения экономических показателей системы тягового электроснабжения. Таким образом, в результате модернизации должна появиться современная тяговая подстанция, удовлетворяющая всем требованиям и показателям качества электроснабжения.

Структурно систему можно представить в виде трёх уровней управления и каналов связи и средств сопряжения между уровнями.

К верхнему уровню (АРМы ЦДП, сервера хранения данных) относятся программные и аппаратные средства, предназначенные для:

- предоставления необходимой информации операторам и энергодиспетчерам в ЦДП, поступающей на мониторы ПК в виде анимации видеокадров, сообщений, видео и звуковой сигнализации;
- сохранения полученной информации в виде архива данных с возможностью его последующей обработки и анализа;
- обеспечения бесперебойного функционирования ПТК (достигается посредством использования источников бесперебойного питания и функций горячего резервирования программно-технических средств);
- организации выдачи отчетов, оперативных журналов и другой документации, необходимой для организации эффективного управления технологическим объектом.

К среднему уровню относятся программные и аппаратные средства (ПК оператора на ТП, шкаф управления подстанцией: сенсорный монитор, контроллер ТП MicroPC, контроллер ОПС), предназначенные для:

- организации физического интерфейса с технологическим оборудованием;
- получения информации от сигнализирующих и измерительных устройств;
- предварительной обработки и передачи полученных сигналов на верхний уровень;
- получения заданных значений и команд от оборудования верхнего уровня;
- реализации алгоритмов локального управления на базе полученных заданий, команд и входных сигналов с выдачей управляющих сигналов на исполнительные устройства.

Эти функции выполняются непосредственно на контролируемом объекте (ТП).

Нижний уровень включает в себя датчики (измерительные преобразователи) контролируемых величин, блоки цифровой релейной защиты и автоматики, функциональные контроллеры.

К средствам сопряжения и связи относятся программные и аппаратные средства, предназначенные для организации своевременной и достоверной передачи информации между уровнями. Это программируемые логические контроллеры, устройства удаленной передачи данных, оптические и медные кабели, каналы связи RS-485, RS-232, Ethernet.

Основой для построения системы является структурная схема шкафа управления подстанцией (рисунок 5). Он является центральным звеном, которое обеспечивает связь между верхним и нижним уровнями системы.

- динамическое отображение на АРМ информации о состоянии коммутационного оборудования;
- динамическое отображение на АРМ текущих значений аналоговых величин и состояний дискретных сигналов, контролируемых блоками ЦРЗА и УСО;
- отображение на АРМ информации о пусках и срабатываниях блоков ЦРЗА;
- отображение на АРМ параметров аварийных событий и осциллограмм, зарегистрированных блоками ЦРЗА, УСО и РАПС;
- просмотр полученной от блоков ЦРЗА и УСО информации в табличных и графических формах, в виде мнемосхем, ведомостей событий, аварийно-предупредительной сигнализации;
- дистанционное чтение и редактирование конфигурации ЦРЗА и УСО (уставки, ключи и т.д.);
- дистанционное управление положением коммутационного оборудования (включение/отключение выключателей и др.);
- ведение долговременного архива событий комплекса, журнала действий операторов и другой вспомогательной информации.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств: учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Схиртладзе А. Г. Автоматизация технологических процессов и производств: учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. — 2-е изд. — Саратов : Ай Пи Эр Медиа, 2019. — 459 c. — ISBN 978-5-4486-0574-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83341.html. — Режим доступа: для авторизир. пользователей.

УГРОЗЫ, СВЯЗАННЫЕ С РАЗВИТИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Белов Ярослав Михайлович, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Московский университет Министерства внутренних дел Российской Федерации имени В. Я. Кикотя , г. Москва

В настоящее время происходит интенсивное развитие процессов информатизации, которая затрагивает практически все сферы жизнедеятельности человека и аппарата управления. Данная тенденция приводит к формированию новой информационной инфраструктуры, под действием которой появляются новые общественные отношение, регулирование которых не успевает за ходом внедрения информационно-телекоммуникационных технологий в жизнь.

Информационно-телекоммуникационные технологии на данный момент решает следующие задачи:

Электронный обмен данными;
Электронный бизнес;
Удалённое обслуживание клиентов;
Электронная почта;
Высокоскоростная передача пакетов данных;
Внутризоновая, международная связь;
Средства массовой информации;
Предоставление досуга, видеохостинг.

Согласно статистических данных, представленных Федеральной службой государственной статистки, в 2011–2018 гг. в России наблюдался активный рост числа абонентов широкополосного доступа к интернету (ШПД) в расчете на 100 человек населения. По фиксированному интернету прирост составил 76%, мобильному – 80%. За последние 11 лет число абонентов фиксированного ШПД увеличилось в 6 раз. [1]

По данным Международного союза электросвязи, в 2018 г. в мире на 100 человек населения приходилось 14.1 абонента фиксированного и 69.3 – мобильного интернета. [2]

Согласно данным Международного союза электросвязи, в 2018 г. интернетом пользовался каждый второй житель Земли (51.2%). Аудитория интернет-пользователей в России также ежегодно увеличивается. Более двух третей (69%) россиян в возрасте 15–74 лет пользуются им ежедневно, еще 11% – не реже одного раза в неделю.

Согласно статистическим данным, полученных в ходе опроса граждан, который проводил Национальных исследовательский университет Высшая школа экономики, был получен результат, что готовность населения к дистанционным операциям, связанным с финансовыми услугами, в России составляет 40%. [3]

По данным приведённым в Единой межведомственной информационно-статистической системе, среди российских пользователей интернета доля столкнувшихся с угрозами информационной безопасности 27.9% в 2018 г. Основными проблемами остаются несанкционированная рассылка, или спам (с ним сталкивались 19.7% взрослого населения, выходившего в сеть), а также заражение вирусами, приведшее к потере информации и/или времени на удаление (8.9%). [4]

Развитие информационно-телекоммуникационных технологий изменяет вектор преступности в целом. Преступления «уходят с улиц» и переходят в сферу «анонимности», согласно последним данным, а именной краткой характеристики состояния преступности в Российской Федерации за январь-февраль 2021 года, выпущенной Министерство внутренних дел Российской Федерации 19 марта 2021 года, за два месяца текущего года в Российской Федерации зарегистрировано на 29,4% больше IT-преступлений, чем год назад, в том числе совершенных с использованием сети «Интернет» – на 48,3% и при помощи средств

мобильной связи – на 32,6%. Если в январе-феврале 2020 года удельный вес преступлений в IT-сфере составлял 19,3%, то за первые 2 месяца текущего года он увеличился до 26,3%. [5]

Это и обуславливает некоторые общие тенденции развития современным информационно-телекоммуникационных технологий, такую как конвергенция и ликвидация промежуточных сведений от источника информации к её потребителю.

Первая тенденция говорит об исчезновении различия между промышленными изделиями и услугами, информационным продуктом и средствами его получения. Происходит диверсификация видов деятельности предприятий, взаимопроникновение различных отраслей промышленности, финансового и торгового секторов, сферы услуг. Объединение разноуровневых компьютерных сетей, обеспечивающих обработку информации.

Вторая заключается в разработке новых методов преобразования информации в удобные и доступные формы для немедленного использования потребителем, тем самым ликвидирует промежуточные звенья производства и ускоряет получение, передачу или отправку документации, денежных средств и тому подобное.

Для понимания этого, можно посмотреть в приложения своего смартфона и увидеть там приложение мобильного банка, портала государственных услуг Российской Федерации и другие приложения, позволяющие быстро совершить какую-либо операцию, используя лишь один телефон и подключение к сети Интернет.

Однако данное удобство и просто для пользователя приводит и к угрозе его безопасности, которая включает в себя незаконное собирание, распространение персональных данных и мошенничество в сфере компьютерной информации.

Нарушение безопасности происходит совершения компьютерных атак, которые можно разделить на сами компьютерные атаки, они в свою очередь будут включать атаки на информационную инфраструктуру Российской Федерации, атаки с использованием программ-шифровальщиков, атак типа «отказ в обслуживании», и атаки с использованием социальной инженерии.

Для недопущения нарушения безопасности при работе с информационно-телекоммуникационными технологиями предлагаю использовать ряд методических рекомендаций.

По предотвращению компьютерных атак:

1. использование антивирусного программного обеспечения на компьютерах пользователей и серверах, а также своевременное обновление его баз;
2. регулярный мониторинг и установка исправлений (патчей) безопасности распространенного офисного программного обеспечения и операционных систем;
3. регулярное обновление сигнатур для систем IDS/IPS и подписок идентификации и анализа киберугроз (Threat Intelligence) для своевременного детектирования подозрительного трафика и поведения;
4. своевременный вывод из эксплуатации неподдерживаемого производителем программного обеспечения в случае наличия такой возможности;
5. проведение политики ограничения использования учетных записей с повышенными привилегиями, ограничение количества учетных записей локальных администраторов;
6. использование паролей, соответствующих требованиям безопасности;
7. исключение хранения в открытом виде;
8. выполнение всех рекомендаций по работе с вложениями, пришедшими из подозрительных источников, в том числе рекомендаций не открывать вложения – исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя;
9. отказ в подтверждении доступа, вызывающих сомнение программ.

По противодействию атакам с применением социальной инженерии:

1. не переходите по неизвестным ссылкам, не перезванивайте по сомнительным

номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках;

2. никому не сообщайте персональные данные, а уж тем более пароли и коды;
3. не храните данные карт на компьютере или в смартфоне;
4. не доверяйте всей получаемой информации, проверяйте её;
5. установите и обязательно обновляйте антивирусные программы на всех используемых устройствах.

Список использованных источников

1. Федеральная служба государственной статистки // Росстат URL: https://rosstat.gov.ru/search?q=информационно+телекоммуникационные+технологии (дата обращения: 28.03.2021).
2. Международный союз электросвязи // МСЭ URL: https://www.itu.int/itu-d/sites/statistics/ (дата обращения: 28.03.2021).
3. Институт статистических исследований и экономики знаний // НИУ ВШЭ URL: https://issek.hse.ru/ (дата обращения: 28.03.2021).
4. Единая межведомственная информационно-статистическая система // ЕМИСС URL: https://rosstat.gov.ru/emiss (дата обращения: 28.03.2021).
5. Краткая характеристика состояния преступности в Российской Федерации за январь-февраль 2021 года // МВД РФ URL: https://мвд.рф/reports/item/23447482/ (дата обращения: 28.03.2021).

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ КОЗЛОВОГО КРАНА

Грачева Римма Александровна, студентка 2 курса
Научный руководитель Горюнова Марина Владимировна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО «Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Грузоподъемные краны занимают ведущее место в системе машин для механизации сортировки и погрузочно-разгрузочных работ в производстве. С помощью грузоподъёмных кранов достигаются высокие темпы и индустриализации производства. Объектами применения таких машин являются практически все цеха с потребностью перемещения крупногабаритных грузов и пункты грузопереработки (склады и др.).

Козловые краны относятся к машинам цикличного действия, так как их рабочий процесс состоит из отдельных чередующихся циклов, включающих рабочие и вспомогательные периоды. Они обеспечивают обслуживание большой площадки рабочей зоны, равной двойному вылету и ходу грузовой тележки, умноженными на длину подкрановых путей. Для увеличения мобильности кранов применяются современные способы их монтажа, демонтажа, транспортирования, подготовки к эксплуатации.

Целью исследования является описание технических параметров автоматизированной системы управления козлового крана.

Задачи исследования:

– предоставить общие сведения о козловом кране;

– описать технологические параметры козлового крана;

– проанализировать устройство и принцип работы автоматизированной системы управления козлового крана.

Объектом исследования является козловой кран.

Предметом исследования является автоматизированная система управления козлового крана.

Основными элементами рабочего процесса, осуществляемого при работе крана, являются:

- приведение технологического процесса управления пусковыми устройствами козлового крана в соответствие с действующими нормативными документами;

- реализация алгоритмов автоматической проверки работы оборудования и пусковых устройств;

- повышение экономичности работы оборудования за счет оптимизации нестационарных режимов работы и сокращения времени пусковых операций.

Козловые крюковые краны общего назначения предназначены для выполнения подъёмно-транспортных, погрузо-разгрузочных и складских работ со штучными грузами. Козловые краны общего назначения обслуживают открытые площадки практически всех типов промышленных предприятий, железнодорожные станции, склады и другие производственные объекты[3].

Козловые краны общего назначения получили наибольшее распространение и отличаются от мостовых кранов тем, что опираются на крановый путь с помощью опорных стоек. Краны данного типа, как правило, исполняются с двухстоечными опорами, причём одна из опор может жёстко соединяться с мостом, а другая - шарнирно. В некоторых случаях рельсовый путь укладывают на разных уровнях при различной высоте опор.

Козловой кран состоит из следующих элементов:

металлический мост;

тележка, установленная или подвешенная на мосту и способная по нему передвигаться;

– две опоры, каждая из которых включает одну или две стойки;

– платформы опор для передвижения по подкрановому пути;
– механизм подъёма груза;
– механизм передвижения тележки;
– механизм передвижения крана.

На рисунке 1 представлен общий вид козлового крана.

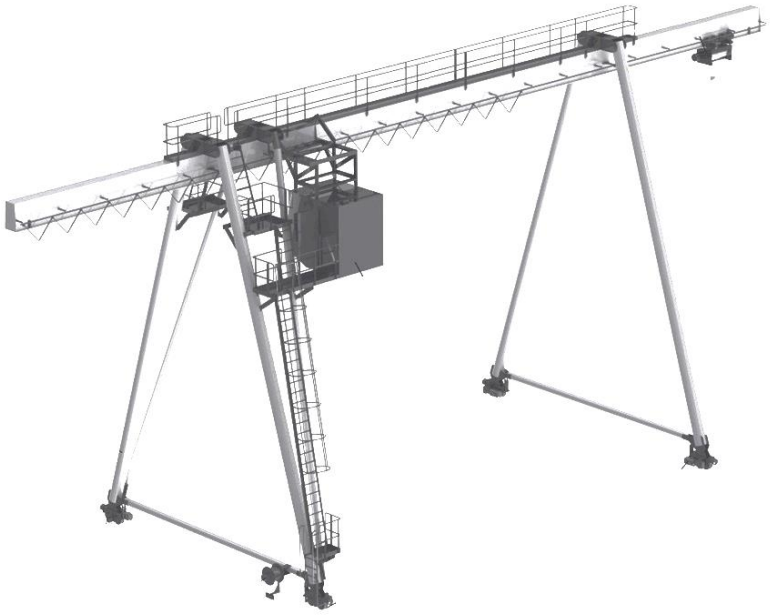


Рисунок 1 - Общий вид козлового крана

Козловой кран выполнен в виде пролётного сооружения, в котором пролётные строения перемещаются по рельсам, проложенным на бетонном фундаменте. Конструкция козлового крана состоит из однобалочного или двухбалочного моста с одной или двумя консолями, или без консолей. Широкое распространение получили однобалочные мосты трёхгранного и четырёхгранного сечения с ездовым монорельсом. Пролетные балки двухбалочных мостов по своей конструкции аналогичны балками мостовых кранов.

Пространственные стойки жёстких опор козловых кранов выполняют трёхгранными или четырёхгранными, при этом их пояса для обеспечения жёсткости связываются диафрагмами или решётками. Механизмы передвижения козловых кранов общего назначения выполняются с раздельным приводом опор.

Привод механизмов подъёма груза и передвижения тележки может быть установлен непосредственно на грузовой тележке (самоходные тележки) или стационарно на мосту (тележки с канатной тягой). При необходимости грузовая тележка комплектуется крюковой траверсой и электроталью вспомогательного подъёма.

В кранах большей грузоподъемности применяются монорельсовые или двухрельсовые, канатные и самоходные тележки. При этом двухрельсовые тележки могут быть подвесными или опорными, перемещающимися по рельсам, уложенным на верхние пояса балок моста.

Управление всеми механизмами крана осуществляется из кабины управления, а работа всех крановых механизмов осуществляется индивидуальными приводами всех рабочих органов. При больших пролётах, когда наблюдение оператора за работой крана затруднено, кабину выполняют перемещающейся совместно с грузовой тележкой.

Система управления с помощью пускорегулирующей электроаппаратуры позволяет контролировать скорость выполнения крановых операций, в частности: перемещение крана, перемещение грузовой тележки и подъём и опускания крюка.

Мост представляет собой пространственную конструкцию разнообразной формы в зависимости от варианта исполнения. Пролет моста может иметь одну или две консоли или не иметь их совсем.

Опоры могут быть одно- или двухстоечными. Они устанавливаются на рельсы, по которым происходит перемещение крана. Также рельсы имеют небольшие зазоры для теплового расширения при длительной работе установки[4].

Кабина оператора размещается в консоли вместе с подъемно-силовыми установками, редукторами и другим оборудованием.

Тележка в козловом кране предназначается для непосредственного перемещения грузов. Она имеет прочную конструкцию. Снабжается редукторами и двигателями.

В качестве устройства подъема применяется крюк, грейфер иди сходное оборудование в зависимости от типа захватываемого груза. Для повышения тяговых характеристик оснащается полиспастом. Также может использоваться магнитный захват в металлообрабатывающих предприятиях.

Механизмы главного и вспомогательного подъема устроены в виде барабанов - лебедок с двумя приводными моторами и с планетной коробкой передач.

Разработка новой автоматизированной системы управления, включающая современные технические средства контроля и управления приводами, позволит выполнять работу механизмов с большей степенью точности.

Автоматизация бывает частичной либо комплексной. Проводится она в соответствии с принятым планом модернизации производства. Любое промышленное предприятие предполагает использование крупногабаритных грузоподъемных кранов.

Для автоматизации управления такими машинами, необходимо сосредоточить внимание на отдельных операциях:

- запуске, торможении механизмов;
- подборе оптимальной скорости рабочих движений;
- фиксации частей крана в нужном положении и так далее.

Для решения подобных задач созданы командоконтроллеры и автоматизированные устройства безопасности - ограничители крайних положений и грузоподъемности, грузозахваты, противоугонные средства. Даже частично автоматизированный кран отличается повышенной производительностью. Такая машина быстрее выполняет работу и требует меньшего количества обслуживающего персонала при перемещении груза.

Необходимость автоматизации управления кранами возникает в том случае, если ввиду напряженности производственного цикла человек попросту не успевает контролировать их работу.

Полная автоматизация актуальна для предприятий, выпускающих изделия серийно и массово. В таком случае всеми операциями управляет компьютер. Для отдельных видов грузоподъемного оборудования (грейферных кранов, подвесных конвейеров, штабелеров) задействуют электромеханические выключатели[2].

Сложные строительно-монтажные работы (СМР), предполагающие применение башенных, мостовых, самоходных, стреловых пневмоколесных и гусеничных кранов, а также перемещение нестандартных грузов, не могут подвергаться полной автоматизации.

Для них необходимо введение обратной связи и следящих систем, что ведет к удорожанию эксплуатации кранов. Основным методом частичной автоматизации СМР является перевод кранов на радиоуправление. При этом подключение средств радиоуправления к электроприводу осуществляется без изменения их характеристик.

Системы радиоуправления грузоподъемными кранами получили широкое распространение на производственных предприятиях, строительных площадках, используются для обслуживания складских помещений, доков, сборочных цехов, сервисных центров.

Применения системы дистанционного управления, позволит увеличить скорость проведения работ, уменьшить временные потери, обеспечить высокую точность операций с грузом на удаленном расстоянии. Удобство и безопасность. Повышение производительности. Сокращение численности обслуживающего персонала. Одновременное управление несколькими кранами с одного пульта дистанционного управления краном.

Радиоуправление кранами (два и более) расположенными в одном цеху. Также возможность привязать управление каждого узла грузоподъемного механизма к определенному пульту. Например, раздельное радиоуправление тельфером и перемещением ГПО по подкрановым путям.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Назначение автоматизированной системы управления козлового крана [Электронный ресурс]: http://remcran.ru/articles/article/automation-control-valves/

3. Описание и технические параметры козлового крана [Электронный ресурс]: https://tehnoros.ru/products/gantry_crane/kk/

4. Характеристика и принцип технических средств автоматизации [Электронный ресурс]: http://alfacran.ru/article-ustrojstvo-kozlovogo-krana

РАЗРАБОТКА И МОДЕЛИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ПОВОРОТНОГО СТОЛА ДЛЯ ПОВЕРКИ ЖИДКОСТНЫХ ТЕРМОМЕТРОВ ФБУ «БЕЛГОРОДСКИЙ ЦСМ»

Гришин Кирилл Юрьевич, студент 4-го курса
Научный руководитель Горюнова Марина Владимировна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО «Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Жидкостные стеклянные термометры являются самым простым средством измерения температуры и повсеместно используются во многих сферах деятельности человека, в том числе, промышленности. Из-за такой распространенности их поверка часто носит массовый характер. Однако особенности их конструкции, и отсутствие какой-либо электрической части не позволяют автоматизировать процесс их поверки, используя стандартное метрологическое оборудование. В данном случае необходим более специфический подход, предполагающий использование иного, уникального оборудования.

Поверка жидкостных, стеклянных термометров осуществляется с помощью погружения средства измерения в термостаты или криостаты, воспроизводящие специальную, температурную среду, для точной поверки термометров.

Актуальность исследования заключается в модернизации методов поверки, путем внедрения нового, уникального, оборудования и получения максимальной эффективности за счет замены механического труда человека на работу автоматизированного оборудования.

Целью исследования является разработка и моделирование автоматизированной системы управления поворотного стола для поверки жидкостных термометров.

Задачи исследования:

- предоставить краткую характеристику процесса поверки жидкостных термометров;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующего уровня автоматизации и определить задачи для модернизации системы управления;

Объектом исследования является термостат жидкостный переливной прецизионный серии ТПП-1.

Предметом исследования является поворотный стол с автоматизированной системой управления.

Поверка жидкостных термометров осуществляется согласно ГОСТ 8.279-78 [2].

Операции поверки:

- внешний осмотр;
- определение метрологических параметров;
- определение поправок для термометров;
- определение погрешности для термометров.

При проведении поверки необходимо применять средства поверки, указанные в ГОСТ 8.279-78.

К ним относятся: установка УТТ-6В-МА, криостаты, сосуд Дьюра, нулевой термостат, прибор тройной точки воды, водяные термостаты, масляные термостаты, оловянный термостат, катетометр, лупа с увеличением 2,5-7, ртутный метеорологический барометр, механический секундомер, ледогенератор, твердая двуокись углерода, этиловый ректификованный спирт, этиловый технический спирт, жидкий азот.

Допускается применять другие вновь разработанные или находящиеся в применении средства поверки, прошедшие метрологическую аттестацию в органах государственной или с их разрешения ведомственной метрологической службы, удовлетворяющие по точности требованиям ГОСТ 8.279-78.

Поверяемые и образцовые термометры перед поверкой должны находиться при температуре 20±5 °С не менее 24 ч.

При внешнем осмотре должно быть установлено соответствие термометров следующим требованиям:

- единица физической величины «°С»;
- номер термометра по системе нумерации предприятия-изготовителя;
- товарный знак предприятия-изготовителя.
- год и квартал изготовления;
- отметки «состарен» (для некоторых термометров);
- марки стекла на самом термометре, в свидетельстве о предыдущей поверке или в паспорте и д.р.

Глаз поверителя должен находиться на уровне горизонтальной, касательной к мениску, так, чтобы штрих шкалы в точке отсчитывания был видим прямолинейным.

При поверке в термостате поверяемый термометр погружают в рабочую среду на глубину, указанную на нем. Если указание о глубине погружения на термометре отсутствует, то поверку проводят при высоте выступающего столбика не более 10 мм. В тех случаях, когда невозможно обеспечить требуемую глубину погружения, при измерениях учитывают поправку на выступающий столбик.

После установки вспомогательного термометра выжидают 10 - 15 мин до установления теплового равновесия. Перед началом отсчитывания по поверяемому термометру записывают показание вспомогательного.

При поверке в термостате показания поверяемого термометра отсчитывают после выдержки его не менее 10 мин при температуре не ниже температуры, соответствующей каждой поверяемой отметке, более чем на пятикратное значение цены деления шкалы образцового термометра. Отсчитывание проводят при постоянной температуре или равномерном повышении температуры в термостате.

После измерения в масляном термостате термометры протирают керосином или другим растворителем, а после измерений в оловянном термостате промывают водой.

Отсчитывание выполняют по образцовому термометру, стоящему слева, затем по поверяемым в порядке их установки слева направо и по второму образцовому термометру. Повторные отсчитывания проводят в обратном порядке.

После проведения поверки производится обработка результатов поверки. Где происходит расчет поправок и расчет погрешностей.

Заключительным этапом проведения поверки является оформление результатов поверки.

Результаты периодической ведомственной поверки оформляют соответствующим документом, составленным ведомственной метрологической службой и клеймением.

Термометры, не удовлетворяющие требованиям ГОСТ 8.279-78, к выпуску и применению не допускают.

В отличие от термопреобразователей сопротивления и термоэлектрических преобразователей, имеющих широкие возможности автоматизации, посредствам использования АСПТ (автоматизированная система поверки термопреобразователей), МИТ-8 (многоканальный прецизионный измеритель температуры), МИТ-2, КИТ-1 (калибратор измеритель температуры прецизионный) и т.п., жидкостные термометры не имеют электрической части, что очень сказывается на удобстве снятия измерений, при поверке нескольких термометров в одном термостате. Это в свою очередь может влиять на точность измерений.

В настоящий момент снятие показаний происходит визуально, человеком, что также влияет на точность измерений, особенно при поверке более точных термометров с мелкими шкалами.

Также существует проблема размещения термометров в термостате, т.к. отверстия вставки термостата не позволяют поверять более узкие жидкостные термометры, в том числе

погружные, из-за чего для каждого отдельного типа термометров приходится тратить время на поиск способа размещения термометров.

Автоматизация системы и внедрение нового оборудования в данном случае сможет решить не только проблему замены человеческого труда на работу машин, но и обеспечить удобство эксплуатации и повысить точность результатов поверки.

Задачей системы автоматизированного управления поворотным столом является внедрение нового оборудования и программного обеспечения в процесс поверки, которое:

- повысит эффективность поверки;
- повысит удобство проведения поверки;
- увеличит точность снятия показаний с термометров;
- уменьшит время подготовительных работ по поверке термометров.

Для достижения этих параметров система должна обладать следующими параметрами:

- высокая скорость отклика;
- эргономическая конструкция;
- удобный пользовательский интерфейс;
- наличие обратной связи;

На основании данных задач и параметров был разработан поворотный стол, и система управления им, включающая:

- вставка с поворотным столом;
- униполярный шаговый двигатель, с редуктором;
- элементы подсветки стола;
- драйвер УШД (униполярный шаговый двигатель);
- контроллер управления драйвером УШД;
- пользовательский интерфейс взаимодействия с контроллером;
- веб-камеру для снятия результатов.

Для реализации целей и задач проекта будет разработан специальный поворотный стол, состоящий из вставки с поворотным механизмом, и креплением для термометров и направляющих, для крепления веб-камеры. Также на стол будут установлены светодиоды, для комфортного снятия показаний с термометров.

В связи с целями и задачами работы выбрано программное и аппаратное обеспечение, описанное ниже.

Для разработки программы контроллера и программного интерфейса использованы Arduino IDE и Visual Studio. Для реализации проекта выбран контроллер ATmega168. В качестве электропривода выбран униполярный шаговый двигатель Nema 23.

Для возможности вращения стола к поворотному элементу крепится шаговый двигатель Nema 23, которым управляет специально разработанный драйвер, состоящий из транзисторов КТ972Б, резисторов 10кОм, диодов SF28 и 1N4007, и конденсатора 470мкФ 40В. Эти компоненты подобраны из учета максимально возможного тока и напряжения в цепи, что позволяет оставить определенный запас по току и напряжению для защиты от выхода из строя компонентов и возможности подключения более мощного двигателя. Также драйвер включает в себя блок питания 12 вольт 2 ампера.

База каждого из транзисторов, через резисторы соединяется с контролером ардуино, осуществляющим управление системой. Для выработки управляющих воздействий будет написана специальная программа, с интерфейсом, позволяющим в реальном времени просматривать изображение с веб-камеры, контролировать и выбирать какой из термометров в данный момент повернут к камере, а также позволит достаточно точно определять показания на термометре, используя три направляющих: верхний предел температуры, нижний предел температуры, и положение ртутного столба. Для удобства мониторинга показаний в программе также будет предусмотрена таблица значений, для записи температур, на основе которой в реальном времени строится график изменения температур.

Вывод:

Представленная система автоматизации позволяет значительно повысить эффективность поверки, за счет увеличения удобства, точности, уменьшения трудозатратности, и увеличения скорости проведения поверки жидкостных термометров.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. - 386с.

2. ГОСТ 8.279-78 Государственная система обеспечения единства измерений (ГСИ). Термометры стеклянные жидкостные рабочие. Методы и средства поверки. – М.: Стандартинформ, 2019.-9с.- Текст: непосредственный.

3. Иванов А. А. Автоматизация технологических процессов и производств: учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

4. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

5. Суркова Л. Е. Моделирование систем автоматизации и управления технологическими процессами : практикум / Л. Е. Суркова, Н. В. Мокрова. - Саратов : Вузовское образование, 2019. - 46 c. - ISBN 978-5-4487-0496-3. - Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - URL: http://www.iprbookshop.ru/82692.html. - Режим доступа: для авторизир. пользователей

6. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. - 2-е изд. - Саратов : Ай Пи Эр Медиа, 2019. - 459 c. - ISBN 978-5-4486-0574-1. - Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - URL: http://www.iprbookshop.ru/83341.html. - Режим доступа: для авторизир. Пользователей.

ТЕСЛА И ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

Жиров Даниил Евгеньевич, студент 3-го курса
Научный руководитель Комарова Юлия Викторовна, преподаватель 1 категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

«Человек, который предвидел технологии 20-го века!» — это Никола Тесла. Свою известность он получил благодаря прогрессивным взглядам и умению доказывать их состоятельность.

Шагом к созданию Всемирной беспроводной системы является одно из самых известных и зрелищных изобретений Николы. Катушка Теслы (рисунок 1) является разновидностью резонансной трансформаторной схемы. Использовалось это приспособление для производства высокого напряжения высокой частоты.

Рисунок 1 - Катушка Теслы

Катушка Теслы использует преобразование переменного напряжения 220 Вольт в очень высоковольтное - до миллионов Вольт. В отличие от обычных трансформаторов, преобразующих напряжение плавно и равномерно, в катушке Тесла напряжение постоянно "срывается", порождая мощные выбросы энергии на выходном электроде. [1]

С помощью подстройки части схемы достигается резонанс - явление, похожее на эффект раскачивания качелей: если в нужный момент подталкивать подвешенное сиденье, амплитуда его движений резко возрастает, так как каждая новая порция энергии полностью идёт на её рост.

Тесла разрабатывал свою систему для передачи электроэнергии на большие расстояния без проводов, используя проводимость верхних воздушных слоев атмосферы. Предполагалось наличие и приемного трансформатора аналогичной конструкции, который бы понижал принятое высокое напряжение до приемлемого для потребителя значения. Эта конструкция имела название Башня Ворденклиф.

Технология Николы Тесла нашла себя в наше время..

В Новой Зеландии стартап Emrod разработал метод безопасной и беспроводной передачи электроэнергии на большие расстояния без использования проводов, и работает по внедрению этой технологии на островах со вторым по величине дистрибьютором электроэнергии в стране, Powerco. Emrod подали заявки на патенты, и представили прототип передающих и принимающих трансформаторов в 2019 году. По сути, это открытие миру доступа к энергии с помощью первой коммерчески жизнеспособной технологии беспроводной передачи электроэнергии на большие расстояния.

Совместный проект Emrod и Powerco должен показать свою эффективности, как технологической, так и с коммерческой точек зрения. В рамках проекта планируется передать энергию от солнечной электростанции на Северном острове клиентам, находящимся в нескольких километрах от неё. Электрическая мощность будет передаваться в виде узкого луча микроволн. Это устранит два фундаментальных недостатка в плане Теслы. Один из них заключался в том, как взимать с людей плату за электричество, которое они могут просто "черпать из воздуха". Другой - необходимость преодолеть закон распространения излучения, который утверждает, что сила сигнала обратно пропорциональна квадрату расстояния, которое он прошёл от передатчика. В результате мощность сигнала резко падает даже на коротких расстояниях. Передача мощности узким лучом вместо излучения во всех направлениях помогает свести к минимуму эту проблему. На рисунке 2 представлена модель передачи электроэнергии.

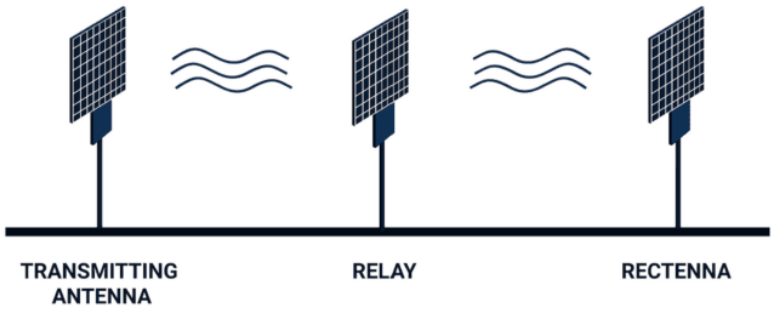


Рисунок 2 - Схематическая модель телеэнергетической системы Emrod

Emrod использует лучи в диапазоне ISM (промышленный, научный и медицинский) с частотами, обычно используемыми в и RfID. Двухточечная передача означает, что мощность передаётся напрямую между двумя точками. Вокруг луча нет излучения, как при передаче по высоковольтному проводу. Маломощная лазерная защитная завеса (система безопасности) гарантирует, что передающий луч немедленно отключится до того, как какой-либо приходящий объект (например, птица или вертолёт) достигнет пространства главного луча, гарантируя, что он никогда не коснется чего-либо, кроме чистого воздуха. Система снижает риск поражения электрическим током, что возможно при проводной передачи электроэнергии.

Технология энергетического излучения, которую использует Emrod, была опробована и раньше, но в основном для военных целей или для использования в космическом пространстве. В 1975 году НАСА использовало микроволновые излучатели для передачи 34 кВт электроэнергии на расстояние 1,6 км. И это всё ещё является рекордом по мощности и расстоянию передачи. По словам основателя Emrod, они будут постепенно увеличивать мощность и расстояние. Важнейшей переменной является эффективность, сейчас это около 60%. Но, чтобы улучшить КПД, у Emrod есть два способа. Один из них - использовать реле. Другой - добавить в приемники так называемые метаматериалы.

Реле, которые представляют собой пассивные устройства, которые не потребляют энергию, работают как линзы, перефокусируя микроволновый луч и отправляя его по своему пути с минимальными потерями при передаче. Они также могут направить его, если необходимо, в новом направлении. Это означает, что передатчик и приёмник не обязательно должны находиться в зоне прямой видимости друг друга.

Метаматериалы - это композиты, содержащие крошечные количества проводящих металлов и изолирующие пластмассы, расположенные таким образом, что они определенным образом взаимодействуют с электромагнитным излучением, таким как микроволны. Они уже используются в так называемых маскирующих устройствах, которые помогают военным кораблям и военным самолётам укрываться от радаров. Но их также можно использовать в приёмной антенне для более эффективного преобразования электромагнитных волн в электричество.

Разработкой систем беспроводной передачи электроэнергии заняты ещё несколько компаний в мире. К примеру, TransferFi из Сингапура, разрабатывает систему, которая формирует лучи радиоволн, которые обычно имеют более низкую частоту, чем микроволны, для передачи мощности конкретным приёмным устройствам, предназначенным для зарядки гаджетов на фабриках, офисах, и в домах.

Американская фирма PowerLight Technologies работает с вооруженными силами над использованием лазеров для передачи энергии на удалённые базы, а также для питания беспилотных летательных аппаратов, когда они находятся в воздухе. Компания также уделяет внимание коммерческим приложениям.

Японская Mitsubishi Heavy Industries изучает возможности использования этой технологии для передачи энергии на Землю с геостационарных спутников, оснащенных солнечными панелями. Для этого потребуется передать его на расстояние более 35 000 км.[2]

Так что мечты Николы Тесла постепенно сбываются. И как электромобили сейчас, через более чем сто лет, стали магистральным путём развития мирового автопрома, так и технология беспроводной передачи электроэнергии также найдёт свое коммерческое применение, и станет элементом повседневной реальности.

Список использованных источников

1. Topor.info [Электронный ресурс]: https://topor.info/hi-tech/izobreteniya-nikolyi-teslyi. Изобретения Николы Теслы, или Мир глазами гения

2. Яндекс. дзен [Электронный ресурс]: https://zen.yandex.ru/media/iap_zts/po-zavetam-i-tehnologiiam-nikoly-tesla-besprovodnaia-peredacha-elektroenergii-na-bolshie-rasstoianiia-uje-realnost-603cd43bd005993399569b13. По заветам и технологиям Николы Тесла - беспроводная передача электроэнергии на большие расстояния уже реальность

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ ВОЗДУХОРАЗДЕЛИТЕЛЬНОЙ УСТАНОВКОЙ ЭНЕРГЕТИЧЕСКОГО ЦЕХА №1 АО «ОЭМК ИМ. А.А.УГАРОВА»

Зыков Виктор Андреевич, студент 4-го курса
Научный руководитель Азарова Виктория Сергеевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

На современном этапе научно-технического прогресса возрастает потребность в продуктах криогенной техники. Расширяются области их применения в народном хозяйстве, и особенно растет необходимость в продуктах разделения воздуха: кислороде, азоте, инертных газах. Основными потребителями кислорода и азота остаются черная и цветная металлургия, химия, нефтепереработка, ракетная техника.

В связи с этим на современном уровне развития криогенной техники проблемы снижения затрат на производство продуктов разделения воздуха, энергозатрат и материалоёмкости, а также повышение надёжности установок следует рассматривать как комплексную межотраслевую проблему.

Целью исследования является расширенный анализ АСУ воздухоразделительной установки АО «ОЭМК»

Задачи исследования:

- изучить характеристику технологического процесса воздухоразделительной установки;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектами исследования являются кислородная станция и участок компрессии АО «ОЭМК».

Предмет исследования - автоматизированная система управления воздухоразделительной установкой АК-15П АО «ОЭМК».

Объектом автоматизации является воздухоразделительная установка АК-15П АО «ОЭМК». Данная установка является энергетической, в процессе эксплуатации которой с высокой динамикой изменяются связанные между собой технологические параметры.

Назначение воздухоразделительной установки АК-15П - производство газообразного чистого азота и газообразного технического кислорода, возможно получение жидких азота или кислорода (или газообразного кислорода высокого давления).

Воздухоразделительная установка представляет собой комплекс устройств, размещенных в специальных помещениях и предназначенных для разделения воздуха на его составляющие [1].

Основными элементами воздухоразделительной установки являются ректификационная колонна, турбодетандерные компрессоры и атмосферные испарители. К вспомогательным устройствам относятся фильтры, резервуары, криогенные насосы и холодильные камеры.

Одним из важнейших процессов, происходящих в воздухоразделительной установке, является разделение воздуха. Воздух после сжатия в компрессоре проходит блоки очистки, где освобождается от влаги, углекислоты и углеводородов, расширяется в детандере с понижением температуры, проходит через теплообменники, сжижается и попадает в ректификационную колонну на разделение, после чего, в зависимости от режима, выдается азот или кислород в жидком или газообразном состоянии.

Схема автоматики регулирования и контроля установки предусматривают следующие системы:

– Измерение температуры термометрами сопротивления ТСП.

– Измерение давления на трубопроводах и заслонках.

– Измерение расхода на манометрах дифференциальных типа ДМ-2010.

– Контроль технологических процессов ведется по показаниям самопишущих приборов КСМ-2, КСД-2, КПД-21.

– Система блокировок, защит и сигнализации выполнена на электромагнитном реле.

В кислородной станции применяются:

1) измерительные преобразователи ДМ-2010, предназначенные для работы в системах автоматического контроля, регулирования и управления технологическими процессами и обеспечивают непрерывное преобразование значения измеряемого параметра: давления газа и воздуха, расход охлаждаемой воды через блок охлаждения, расход газа в выходной сигнал по напряжению;

2) механизмы исполнительные электрические однооборотные постоянной скорости МЭО-25, предназначенные для перемещения регулирующих органов в системах автоматического регулирования технологическими процессами в соответствии с командными сигналами автоматических регулирующих и управляющих устройств.

На щит в операторной комнате также выведены: температура сетевой воды после котла, температура сетевой воды перед котлом, температура дымовых газов, которые регистрируются на приборах серии КСП-2 или КСМ-3 [4].

Система автоматики регулирования и контроля колонны разделения:

- Автоматическое регулирование подачи воздуха и газа;
- Система автоматического контроля температуры газа на выходе из колонны;
- Система автоматического разделения газа.

В результате анализа существующего уровня автоматизации были выявлены следующие недостатки:

- увеличение стоимости системы автоматизации из-за необходимости применения более дорогих приборов и клапанов, поддерживающих обмен данными по полевой шине, и установки специализированного коммуникационного оборудования;
- снижение отказоустойчивости за счёт подключения всех устройств в пределах сегмента к одному кабелю (при его повреждении происходит потеря связи со всеми устройствами сегмента);
- невозможность решения вопросов связи УВК с приборным, электротехническим оборудованием и клапанами с использованием только полевых шин в связи с ограниченным набором оборудования, поддерживающего эти способы обмена данными.

Для модернизации АСУ предлагается:

- обеспечение безопасного технологического режима;
- повышения качества и быстродействия регулирования, и достижение высокого уровня стабилизации технологических режимов;
- увеличение выдачи жидкого кислорода с одновременным производством газообразного азота.

Для решения поставленных задач необходимо выбрать:

- датчики давления «Сапфир»;
- приводы управляемых арматур фирмы «Камоцци Пневматика»;
- контроллер фирмы «Сименс» S7-1500 с языком программирования «Step7» [3].

Модернизация автоматической системы управления АСУ воздухоразделительной установки АО «ОЭМК» заключается в экономии ресурсов производства и повышении надежности системы управления.

Таким образом, внедрение разработки позволить решить следующие задачи:

- повысить качество технологического процесса;
- заметно сократить аварийные ситуации;
- сократить расход газа.

Список использованных источников

1. Беляков В.П. Криогенная техника и технология. 2008 год.

2. Епифанова В.И. Разделение воздуха методом глубокого охлаждения. М: Машиностроение, том 1, 2007 год.

3. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

4. Кривошеев В.П. Моделирование динамических характеристик сложных объектов управления на примере этиленовой ректификационной колонны // сб. статей V международной заочной научно-технической конференции. Ч. 1 – Тольятти: Изд-во: ПВГУС, 2015. – С. 324–330.

5. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М.: ФОРУМ, 2017. - 224 с.

6. Оскольский электрометаллургический комбинат [Электронный ресурс]: https://www.metalloinvest.com/business/steel/oemk/

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ ТАРЕЛЬЧАТОГО ГРАНУЛЯТОРА ФОК АО «ЛГОК»

Игнатьева Валерия Андреевна, студентка 4-го курса
Научный руководитель Хархота Надежда Васильевна, преподователь
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Существенное преимущество гранулированного продукта по сравнению с сыпучим материалом объясняет широкое распространение данного процесса в промышленности. Гранулы легко транспортируются, не загрязняют окружающую среду пылью, просто дозируются, не выветриваются и не слеживаются. Грануляторы предназначены для получения гранул из порошкообразных материалов с добавлением жидкофазного связующего.

Целью исследования является расширенный анализ АСУ тарельчатого гранулятора ФОК АО «ЛГОК».

Задачи исследования:

- изучить характеристику технологического процесса гранулирования и технологические параметры тарельчатого гранулятора;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является тарельчатый гранулятор ФОК АО «ЛГОК».

Предмет исследования автоматизированная система управления тарельчатого гранулятора ФОК АО «ЛГОК».

Фабрика окомкования- цех по производству обоженных окатышей АО «ЛГОК».

Тарельчатые грануляторы представляют собой разновидность оборудования для гранулирования различного материала. Основным назначением является получение сферических гранул определенного размер из порошкового материала путем окатывания.

Управление технологическим процессом, пуск оборудования и контроль за его работой осуществляется централизованно операторами с пультов управления. На фабрике имеются операторские пункты: в корпусе шихтоподготовки, в корпусах окомкования и обжига 1 и 2 и в корпусе обожженных окатышей.

Для централизованного управления механизмами применяются системы УПТС-К и Поток - М, обеспечивающие условия безопасной эксплуатации технологического оборудования.

Все основные технологические операции получения и термообработки окатышей полностью или частично автоматизированы.

Объем автоматизации представлен двумя видами систем:

- системой автоматического контроля, сигнализации и защиты;
- системой автоматического регулирования.

Система автоматического контроля, сигнализации и защиты выполнена на базе контроллерного оборудования фирмы «Сименс», первичных датчиков фирмы «Сименс» и отечественного производства, станций визуализации (управления) на базе IBM совместимых компьютеров.

В состав цепи окомкования входят:

– загрузочные бункеры шихты;
– дисковые питатели;
– конвейеры загрузки шихты в окомкователи;
– конвейеры транспортировки сырых окатышей на сборные конвейеры загрузки обжиговой машины;

– грохота сырых окатышей;

– трубопроводы, обеспечивающие подачу смазки, воды, воздуха к оборудованию.

Структурная схема системы экстремального регулирования шагового типа приведена на рисунке 1.

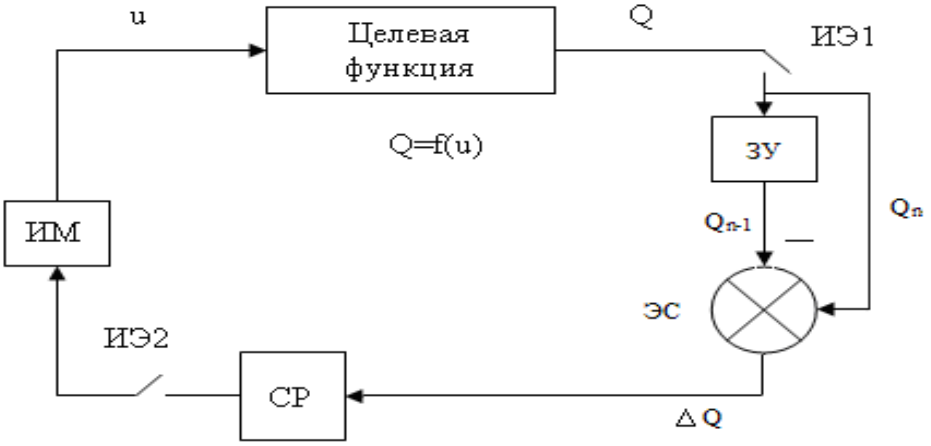


Рисунок 1 - Система экстремального регулирования шагового типа.

Изменение выходной величины объекта Q в системе происходит дискретно (за счёт наличия импульсного элемента ИЭ, расположенного за датчиком выхода объекта), через определённые промежутки времени Δt. Значения Qn подаются на запоминающее устройство ЗУ (элемент запаздывания).

Запоминающее устройство подаёт на элемент сравнения ЭС предыдущее значение Qn-1. На элемент сравнения одновременно поступает Qn, при этом на выходе получается сигнал равный ΔQ выхода объекта за отрезок времени Δt. Если ΔQ<0, то сигнум-реле срабатывает и меняет направление изменения сигнала входа u, иначе направление остаётся прежним.

Существующая система управления технологическими процессами не удовлетворяет современным требованиям по уровню автоматизации и степени защиты технологического оборудования, а именно:

Используемая система щитового управления, которая значительно уступает по всем показателям системам управления с использованием автоматизированных рабочих мест (АРМ) на базе персональных компьютеров.

Применяемые пневматические контрольно-измерительные приборы и средства автоматизации устарели как морально, так и физически, что не позволяет обеспечить необходимые точность измерений, время принятия решений, скорость управления, а также степень надежности работы системы управления.

Низкий уровень автоматизации и неэффективная работа автоматики ведут к неоправданному износу технологического оборудования и нерациональному расходованию всех видов производственных ресурсов, оказывают негативное психофизиологическое воздействие на обслуживающий персонал ввиду того, что основная нагрузка по принятию решений о переключениях регулирующих органов, исполнительных механизмов, контроля за средствами КИПиА падает на операторов, что может привести к ошибкам операторов, привести к нарушениям технологического процесса и выводу оборудования из строя.

Основные недостатки системы автоматизации:

1. Случайные возмущения, действующие на объект во время работы системы регулирования, могут приводить к дрейфу экстремальной характеристики, что существенно затрудняет поиск экстремума и даже могут привести систему в неустойчивое состояние.

Особенно влияние помех сказывается в области экстремума, где изменения целевой функции (ЦФ) в процессе поиска близко к нулю.

2. Увеличение числа параметров участвующих в поиске экстремума существенно затягивает процедуру поиска экстремума.

3. Наличие пробных воздействий, непрерывно посылаемых на объект в процессе функционирования экстремальных систем, обычно неблагоприятно сказывается на режиме эксплуатации промышленных объектов;

4. Сложность в выборе оптимального шага варьирования управляемой переменной.

В связи с отсутствием систем автоматического управления процессом окомкования на тарельчатом грануляторе возникает необходимость исследования объекта управления и возможности автоматического управления процессом окомкования.

В процессе управления окомкователем целью ставиться добиться выхода качественных окатышей при сохранении производительности на некотором постоянном уровне, который коррелирован с производительностью обжиговой машины. При этом необходимо учитывать такие параметры чашевого окомкователя как угол наклона тарели к горизонту, скорость ее вращения, влажность и физико-химические свойства шихты. Последние параметры в свою очередь оказывают решающее влияние на весь процесс окомкования в целом.

Для модернизации АСУ предлагается:

– управление технологическими операциями;

– управление пусками - остановками технологических агрегатов;

– анализ и обобщенная оценка состояния процесса в целом по его модели (распознавание технологических ситуаций, диагностика аварийных состояний оборудования);

– обеспечивать оптимальное управление технологических процессов в установившемся режиме путем автоматического управления;

– оперативный контроль за состоянием параметров технологического процесса;

– контроль состояния механизмов (работает, остановлен);

– формирование и выдачу оперативных и архивных данных о состоянии системы и действиях обслуживающего персонала в реальном масштабе времени;

– организацию обмена данными по сетям (выдача информации в сеть комбината);

– учет технико-экономических показателей;

– система сигнализации о событиях, связанных с неисправностями и нарушениями режимов работы оборудования, отклонениями от норм параметров технологического процесса в реальном масштабе времени, и фиксацию их в архиве;

– аварийное отключение агрегатов в случае возникновения аварийных ситуаций;

– обеспечение блокировочных зависимостей при пусках и остановках механизмов и технологических цепочек;

– программную защиту от несанкционированного вмешательства;

– обеспечение сигнализации перед запуском оборудования и аварийном отключении;

обеспечивать бесперебойное питание средств автоматизации

Для решения поставленных задач необходимо:

– выбрать датчик влажности LB 350 фирмы Berthold

– выбрать исполнительный механизм для контура расхода воды SIPART PS2 фирмы Siemens

– выбрать контроллер SIMATIC S7-1500 с CPU 1513-1 PN

Модернизация автоматической системы управления АСУ тарельчатого гранулятора АО «ЛГОК» заключается в экономии ресурсов производства и повышении надежности системы управлении.

Таким образом, внедрение разработки позволить решить следующие задачи:

– Сократить количество брака;
– Повысить надежность системы управления;
– Повысить качество протекания технологического процесса;
– Экономить ресурсы производства

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Лебединский ГОК [Электронный ресурс]: https://www.metalloinvest.com/ Процессы и производства. Официальный сайт.

ПРОГРАММНЫЕ ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА И ОПТИМИЗАЦИИ ОС

Капцова Наталья Владимировна, курсант 3 курса 981 взвода ФПСОИБ
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В современности сложно представить человечество без использования современных технологий. Их использование зачастую невозможно без эксплуатации операционных систем. Соответственно, операционные системы являются ключевым инструментом для решения любых задач, связанных с информационными технологиями. Для успешного решения таких задач необходимо, чтобы система отвечала всем современным требованиям, а также чтобы в процессе использования она оставалась сбалансированной в функциональном смысле.

1. Операционные системы

Операционная система (ОС) — это совокупность программных средств, управляющих ресурсами компьютера, запускающих и обеспечивающие их взаимодействие с периферийными устройствами и программами, а также обеспечивающих пользовательский интерфейс. Операционные системы можно разделить на локальные и сетевые.

1.1. Локальные операционные системы

Локальные операционные системы используются на отдельных компьютерах, которые применяются в компьютерных сетях как клиенты. В составе локальных ОС есть клиентская часть программного обеспечения для получения доступа к отдаленным ресурсам и услугам. Локальные ОС имеют немаловажные возможности разделения доступа к информации, ее целостности.

В качестве локальных операционных систем обычно используют 32х и 64 разрядные системы. Самые популярные из них – операционные системы от компании Microsoft, такие как WIndows 7, WIndows 8.1, WIndows 10. Более редкими можно считать Linux и MacOS в различных их версиях и сборках.

Наборы сгруппированных по каким либо типам функций операционных систем называют подсистемами. В качестве наиболее важных подсистемам управления ресурсами можно выделить подсистемы управления памятью, процессами, файлами и периферийными устройствами, а подсистемами, являющимися общими для всех ресурсов, являются подсистемы защиты данных, пользовательского интерфейса, и администрирования.

1.2. Сетевые операционные системы

Сетевые ОС в основном применяются для управления несколькими компьютерами, объединенными в одну сеть. Сетевая операционная система дает возможность пользователю работать со своим компьютером, как с отдельным ПК, так и добавляет еще возможность доступа к информации и аппаратным ресурсам других компьютеров в сети.

В сетевых операционных системах, используемых в наше время существуют различные подходы к организации управления ресурсами сети:

1) таблицы объектов (Bindery). Применяются в сетевых операционных системах таких, как Novell NetWare. Подобная таблица есть на любом файловом сервере. Подобная организация работы подходит для одного сервера;

2) структура доменов (Domain). Все ресурсы сети и пользователи объединяются в группы. Домен является аналогом таблиц объектов, только в этом случае эта таблица общая для объединенных серверов с общими ресурсами;

3) служба наименований директорий или каталогов (Directory Name Services - DNS). Сетевые ресурсы: принтеры, память, пользователи, серверы и т.д. - отдельные части информационной системы. Таблицы, которые определяют DNS, есть на каждом сервере. Это увеличивает надежность системы и облегчает обращение пользователей к ресурсам сети.

При организации работы в сети операционная система имеет роль интерфейса, закрывающего от пользователя все подробности программно-аппаратных

средств сети на самом низком уровне. Например, вместо числовых адресов операционная система компьютерной сети дает возможность работать с удобными для запоминания буквенными именами. В результате для пользователя сеть формируется в очень понятный набор разделяемых ресурсов.

Сетевая система дает пользователю некую «виртуальную» вычислительную систему, с которой удобнее работать, нежели чем с реальной сетевой аппаратурой. Однако эта виртуальная система не совсем прячет распределенную основу своего реального прототипа. При обращении к ресурсам компьютеров сети пользователям сетевой операционной системы необходимо помнить, что они работают с сетевыми ресурсами, и для доступа к ним нужно выполнить некоторые отдельные операции.

Пользователям сетевой операционной системы должно быть известно, где хранятся их файлы. Это существенно упрощает использование команд для перемещения файлов с одной машины на другую.

Работая в сетевой системе, пользователь, хотя у него и есть возможность запустить задание на любом компьютере компьютерной сети, всегда знает, на каком компьютере выполняется его задание. По умолчанию пользовательскиепрограммы выполняются на том компьютере, на котором пользователь сделал логический вход.

Сейчас самую большую популярность получили следующие сетевые операционные системы: NetWare фирмы Novell, Windows NT Server фирмы Microsoft и сетевые системы семейства UNIX.

1.3 Основные функции ОС

Основными функциями ОС являются:

− управление оперативной памятью;
− загрузка программ в оперативную память и их выполнение;
− интерфейс пользователя;
− стандартизованный доступ к периферийным устройствам;
− управление доступом к данным на внешних носителях;
− работа с сетью.

Дополнительные функции ОС:

− поддержка многозадачности;
− обмен данными через буфер обмена;
− защита от НСД;
− многопользовательский режим работы.

В состав операционной системы входят три группы компонента:

− ядро с планировщиком; драйверы устройств, управляющие устройствами;
− сетевая подсистема, файловая система;
− системные библиотеки и оболочка с утилитами.

Операционная система Windows - разработанная корпорацией Microsoftоднопользовательская операционная система для персональных компьютеров. Операционная система Windows является многозадачной и поточной, отличается оконным графическим интерфейсом.

1.4 Общие сведения о средствах анализа и оптимизации ОС

Программы диагностики операционных систем должны обладать таким функционалом, как:

− поиск неисправностей работы программного обеспечения;
− поиском аппаратных неисправностей;
− встроенными утилитами для оптимизации системы;
− отказоустойчивостью;
− возможностью обновления таких программ.
− возможностью проверки системы и формирования отчетов о проверке системы.

В пример можно привести программное обеспечение Norton Crash Guard Deluxe (Symantec), Partition Magic (PowerQuest) и Drive Works (Vcom).

Пакеты утилит должны выполнять пять основных задач.

1. Проверка на наличие ошибок, их анализ и пути их исправления, если это возможно.
2. Оптимизация системы при помощи встроенных утилит.
3. Поддержка работы с файлами.
4. Резервное копирование данных системы.
5. Защита от вирусов.

Список использованных источников

1. Большаков Т.В.Операционные системы: учеб. пособие/Д.В. Иртегов; НГУ.- Новосибирск:, 2010-136с.

2.Гук М. Аппаратные средства локальных сетей. Энциклопедия. - СПб.: Питер, 2008. - 576с.

АВТОМАТИЗИРОВАННАЯ СИСТЕМА УПРАВЛЕНИЯ КОНВЕЙЕРАМИ

Козубов Кирилл Александрович, студент 3-го курса
Научный руководитель Комарова Юлия Викторовна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Автоматизация отдельных конвейеров и конвейерных линий производится по двум основным схемам:

- дистанционное управление, при котором автоматизируются только пуск и остановка конвейера;
- автоматизированный контроль за работой конвейера и его элементов, при котором приводные двигатели автоматически отключаются при нарушении режима работы конвейера или его отдельных элементов.

Управление конвейерными линиями в простейшем случае заключается в пуске и останове электродвигателей, приводящих в действие тяговые органы конвейеров. Так как число конвейеров в линии может быть значительным, то применяется централизованное управление приводами конвейерных установок с автоматизированным пуском. В этом случае оператор подает только начальный командный импульс на пуск первого конвейера, а двигатели остальных конвейеров включаются автоматически в заданной последовательности. Тем самым централизованное управление позволяет освободить человека от непосредственного участия в пуске каждого конвейера.

Согласно правилам безопасной эксплуатации, к аппаратуре автоматизированного или дистанционного управления отдельными конвейерами или конвейерными линиями предъявляются следующие основные требования:

- обеспечение подачи предпускового предупредительного сигнала длительностью не менее 5 с;
- включение конвейеров в линию в последовательности, обратной направлению грузопотока, и обеспечение пуска последующего конвейера (против грузопотока) после разгона предыдущего;
- автоматическое одновременное отключение всех конвейеров в линии, транспортирующих груз на вышедший из строя конвейер;
- невозможность повторного включения неисправного конвейера при срабатывании электрических защит электродвигателя механической части конвейера и др.;
- отключение провода из любой точки по длине конвейера и наличие местной блокировки, предотвращающей пуск данного конвейера с пульта управления;
- возможность перехода на местное ручное управление приводами отдельных конвейеров при ремонте, осмотре и регулировании.

Аварийное отключение привода конвейера должно осуществляться при обрыве ленты, затянувшемся пуске, снижении скорости ленты до 75% от номинальной, завале перегрузочного пункта и т.д. Между пультом управления, местом расположения приводов конвейера и пунктами загрузки конвейерной линии должна быть двухсторонняя телефонная связь или кодовая сигнализация.

Автоматизированная система управления конвейерами и конвейерными линиями АСУК-ДЭП

Система «АСУК-ДЭП» предназначена для автоматизированного управления разветвленными и неразветвленными конвейерными линиями, а также одиночными конвейерами, входящими и не входящими в состав конвейерной линии, в подземных выработках шахт и рудников, а также в поточно-транспортных системах поверхностного комплекса (на обогатительных фабриках, во вспомогательных цехах и др.).

По технической реализации АСУК-ДЭП не уступает существующим сегодня в мировой горнодобывающей промышленности аналогичным системам. Например, АСУК-ДЭП полностью заменяет аппаратуру автоматизации АУК-10ТМ и может функционировать со всеми теми же датчиками, но имеет значительно более широкие возможности.

Система допускает управление конвейерами с числом двигателей до четырех и с нерегулируемой скоростью рабочего органа, производит мониторинг и архивацию технологических параметров.

Система является проектно-компонуемой, т.е. количественный и качественный состав оборудования, топология сетей передачи данных, типы каналообразующего оборудования, а также функциональность и состав оборудования диспетчерского уровня определяются в ходе рабочего проектирования, на основе утвержденного Заказчиком технического задания.

Подземная часть системы АСУК-ДЭП реализована на базе взрывобезопасного комплекса ДЕКОНТ-Ex. Наземная часть – на базе комплекса ДЕКОНТ общепромышленного исполнения.

Основные функциональные характеристики:

- Запуск конвейерных линий, их частей, а также дозапуск без остановки работающих конвейеров в последовательности, исключающей завал мест перегрузок, контроль скорости ленты и пробуксовки;
- Оперативный останов конвейерной линии, части линии, отдельного конвейера (с автоматическим отключением всех конвейеров, подающих груз на остановившийся) по командам с АРМ диспетчера или по командам с блока управления конвейером (с обеспечением необходимой последовательности включения и отключения механизмов конвейера);
- Управление звуковой сигнализацией конвейера, конвейерной линии (предупредительная, аварийная, вызывная, др.);
- Местное автоматизированное управление конвейером, осуществляемое с блока управления конвейером;
- Обеспечение различных видов защит (аварийный и экстренный останов): экстренный останов с любого места конвейера, при сходе ленты, при снижении скорости и пробуксовке, при срабатывании датчика заштыбовки, при съеме ограждения, при срабатывании датчика температуры приводного барабана, др.;
- Останов по взаимоблокировке конвейерной линии, части линии или отдельного конвейера;
- Отключение фидерного автоматического выключателя при залипании блок-контактов электродвигателей или при залипании блок-контактов тормозов;
- Отображение информации на БУК и на АРМ диспетчера:

1. оперативная индикация о режиме работы, скорость ленты и др.;
2. аварийная индикация всех видов защитных отключений и блокировок;
3. первопричины последнего останова конвейерной линии, части линии, отдельного конвейера;
4. оперативное отображение на АРМ диспетчера состояний управляемых объектов.

- Определение адреса при срабатывании датчиков в шлейфах КТВ и КСЛ;
- Архивация технологических параметров, протоколирование действий диспетчера;
- Настройка системы в процессе эксплуатации. АСУК-ДЭП имеет возможность изменения в процессе эксплуатации как настроек, общих для всех конвейеров в линии, так и индивидуальных на каждый конвейер (таймауты и уставки), исключая несанкционированный доступ. Параметры каждого конвейера, а также факты их изменения сохраняются в архиве с возможностью последующего просмотра.

Для обеспечения надежной и безопасной работы конвейерных установок используется большое число различных средств автоматического контроля и защиты.

Реле скорости типов РСА, УКС, КДК контролируют скорость тягового органа конвейера и его исправность. При обрыве тягового органа реле скорости дает сигнал на отключение электропривода.

Источником сигналов для реле скорости служат тахогенераторные и магнитоиндукционные датчики скорости.

Унифицированное устройство контроля проскальзывания и скорости УКПС контролирует проскальзывание и скорость ленты, сигнализирует о нарушениях нормального режима, выдает команду на управление механизмом натяжения ленты, отключает привод конвейера при аварийных режимах работы. Устройство УКПС состоит из электронного блока БЭ и датчиков контроля скорости.

Датчик скорости контролирует скорость приводного барабана, а датчик – контроль скорости ленты. Выходными сигналами этих датчиков являются импульсы напряжения, частота которых пропорциональна скорости.

Проскальзывание ленты относительно приводного барабана контролируется периодическим измерением разности количества импульсов, поступающих в блок от датчиков приводного барабана и конвейерной ленты. Эта разность пропорциональна разности линейных скоростей приводного барабана и ленты, т.е. проскальзыванию ленты относительно приводного барабана. При отсутствии проскальзывания ленты относительно приводного барабана частоты импульсов от датчиков одинаковы.

Скорость привода конвейера контролируется путем периодического определения количества импульсов датчика за определенное время и сравнения этого количества с заданной величиной. Контроль скорости ленты также выполняется периодическим определением количества импульсов датчика за определенный промежуток времени. Подсчет числа импульсов, поступающих с датчиков скорости, и их сравнение с заданными значениями происходят в электронном блоке.

Датчик контроля схода ленты КСЛ-2 осуществляет контроль аварийного схода ленты в сторону. Датчик состоит из корпуса, гибкого привода и исполнительного устройства. В корпусе расположено исполнительное устройство, состоящее из магнитной системы и геркона, заключенного в капсулу.

При аварийном сходе в сторону конвейерная лента воздействует на гибкий привод. Это воздействие передается на трос, который перемещает кольцевую магнитную систему вдоль капсулы геркона, что приводит к переключению контактов геркона.

Датчик контроля заштыбовки ДЗШ предназначен для контроля мест пересыпов горной массы с конвейера на конвейер, а также для контроля уровня горной массы в бункерах и других загрузочных устройствах. Датчик состоит из шарикового контактного элемента, помещенного во взрывобезопасный стальной корпус, и подвешивается на кабеле, укрепленном стальным тросом. При превышении заданного уровня засыпки датчик отклоняется на угол, достаточный для перемещения шарика. Последний перемещается в сторону и замыкается с контактным кольцом. При уменьшении угла наклона шарик возвращается в исходное положение и контакт размыкается.

Контроль температуры приводных барабанов ленточных конвейеров выполняется аппаратурой АКТЛ-1, которая отключает приводной двигатель при нагреве барабанов выше допустимой температуры (65±10 °С), предотвращая возможное воспламенение ленты при ее пробуксовке. В качестве датчика температуры используется ферритовый термодатчик, являющийся сердечником катушки индуктивности. При нагреве барабана до температуры 65±10 °С резко снижается магнитная проницаемость ферритового термодатчика и соответственно уменьшается индуктивность катушки. Это приводит к появлению сигнала, который отключает цепь управления магнитного пускателя электродвигателя, и конвейер останавливается.

Аппаратура автоматизации орошения АО-3 предназначена для автоматического включения и выключения системы орошения в пунктах перегрузки горной массы с конвейера на конвейер для уменьшения пылеобразования.

В комплект аппаратуры АО-3 входят релейный блок, управляемый вентиль, датчик наличия материалов ДНМ, форсунка. При движении материала на конвейере замыкается контакт датчика ДНМ. Это приводит к включению электромагнитного вентиля и подаче воды к форсунке, установленной над сбрасывающим барабаном конвейера. В случае прекращения движения материала размыкается контакт ДНМ, катушка электромагнитного вентиля отключается, и подача воды прекращается.

Кабель–тросовый выключатель КТВ-2 применяется для сигнализации и экстренного останова из любого места конвейерной линии. Он содержит геркон, на который воздействует поле постоянного магнита. При оттягивании штока, на котором закрепляется кабель-трос, между магнитом и герконом вводится стальной экран, что приводит к размыканию контактов.

Реле времени РВИ-1М используют для создания выдержки времени при пуске мощных подземных конвейеров. Схема реле обеспечивает выдержку времени в диапазонах 0,5 – 300 с.

Список использованных источников

1. https://svc-college.ru/wp-content/uploads/2020/12/Автоматизация-конвейерных-линий.pdf
2. https://allics.ru/services/avtomatizirovannye-sistemy-upravleniya/avtomatizatsiya-konveyerov
3. http://electricalschool.info/main/drugoe/650-cistemy-upravlenija-konvejjerami-i.html

СПОСОБЫ ПРЕДОТВРАЩЕНИЯ КИБЕРАТАК

Коломина Анна Сергеевна, курсант 2 курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.[1]

В современном мире мы все чаще используем слово «кибератака».

Кибератака это массовый взлом компьютерных сетей, либо массовое заражение компьютеров вирусами. Слово «кибер» может означает «компьютерный» или «связанный с интернетом» [1]. Другими словами, атака направленная на носитель данных, специально предназначенный для их хранения, обработки и передачи личной информации пользователя.

Киберпреступность на данный момент становиться самым опасным видом преступности, как для всей мировой экономики, так и для отдельных компаний. Так ущерб мировой экономике от кибератак в 2019 году по всему миру вырос до $2,5 трлн. В 2018 году убытки компаний от кибератак достигли $1,5 трлн — таким образом, за год ущерб от подобного рода преступлений вырос более чем в 1,5 раза. К 2022 году, по прогнозу Всемирного экономического форума, сумма планетарного ущерба от кибератак может вырасти до 8 трлн долларов.[3]Но кибератаки опасны не только в экономической сфере. В начале 2019 года в Германии стало известно о масштабной утечке личных данных немецких политиков. Также в этом же году американский правительственный сайт, на котором публикуется в открытом доступе документация, взломали якобы иранские хакеры и разместили заявления в поддержку Тегерана и против президента США Дональда Трампа. Сообщения о взломах и хакерских атаках появляются регулярно.

Одним из основных негативных факторов кибератак является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Обобщая имеющуюся знания о киберугрозах современности можно сказать, что кибератаки могут осуществляться как одним человеком, так и группой людей. Жертвами таких атак могут стать не только отдельные пользователи, но и организации, компании, государственные органы, политические деятели, политические партии и целые государства. Кибератаки как правило организуются удаленно, поэтому обладают высокой латентностью. В отличии от распространения вирусных атак, кибератаки носят целенаправленный характер. В связи, с чем возникает необходимость борьбы с данным видом противоправных действий.

Первый способ защиты от кибератак предлагают военные организации.

В 2020 году в каждом военном округе сформируют специальный центр по борьбе с кибератаками, рассказали источники «Известий» в Минобороны**.[4]** Их задача —

обеспечение защиты от компьютерных атак, а также защита от вирусов. Центры будут контролировать как открытые военные линии связи и передачи данных, так и защищенные.

В перспективе все киберцентры в округах предполагают объединить в глобальную систему информационной защиты. Они возьмут под охрану трафик Минобороны, поступающий как из сетей гражданских операторов, так и из «военного интернета» — закрытого сегмента передачи данных (ЗСПД). Мониторинг сетей военнослужащие станут вести в круглосуточном режиме.

Сейчас в ВС насчитывается более 180 тыс. пользователей ЗСПД. Для информационного обеспечения армии и флота создан уникальный территориально-распределительный центр обработки данных, к услугам которого ежедневно обращается более 23 тыс. военнослужащих.

ЗСПД, не соединенный с мировой паутиной, начал работу в 2016 году. В нем есть свой электронный почтовый сервис, по которому разрешена передача секретной информации, включая документы с грифом «Особой важности». Основной ресурс сети доступен по адресу mil.zs. Зайти на военные сайты можно через компьютеры, которые сертифицированы службой защиты гостайны.

Мониторинг сетей военнослужащие станут вести в круглосуточном режиме. За поддержание порядка в виртуальном пространстве будут отвечать офицеры, получившие в военных вузах специальность в области информационной безопасности. В случае ЧП дежурной смене предстоит немедленно локализовать угрозу.

Для защиты военной инфраструктуры разработано специальное программное обеспечение, которое обеспечит многоуровневую систему защиты. Первым на пути взломщика встанет «программный» барьер — межсетевой экран. Он сравнивает характеристики входящего трафика с эталонными шаблонами и решает, пропустить или запретить дальнейшее перемещение по сети сообщений или файлов.

В том случае, если вирус проникнет в сеть, его смогут отследить спецпрограммы, которые также позволяют установить место, где это произошло. При обрыве или блокировке одного из каналов передачи электроника в автоматическом режиме предупредит операторов об опасности.

В число основных элементов системы входит и модуль регистрации аварийных сообщений. Он используется для распределения задач по восстановлению связи. Кроме того, офицеры, обслуживающие контур, в режиме реального времени смогут отслеживать трафик и работу сетей. Также им предстоит действовать в тесном контакте со связистами армий, дивизий и бригад.

Второй способ борьбы с кибератаками находится на стадии разработки- квантовая сеть.

Представим такую сеть, которую нельзя взлома, тогда все наши данные будут передаваться без угрозы быть заполучены злоумышленниками.

Первую в России коммерческую линию квантовой связи длиной 670 км построят в 2021 году. Сеть между расположенными в Москве и Удомле (Тверская область) центрами обработки данных обеспечит самую надежную из существующих сегодня степеней защиты информации. Хакеры не смогут взломать ее, какими бы технологиями, включая квантовые компьютеры, не располагали, обещают разработчики. Использовать линию смогут как крупные государственные компании, так и частные корпорации, в том числе банки.[5]

Квантовые коммуникации будут строить на основе уже существующей инфраструктуры ЦОДов, расположенных в Москве и Удомле, и волоконно-оптических линий связи между ними. В этих центрах расположены мощные серверы и сетевое оборудование, предназначенное для обработки, хранения и распространения информации. Сейчас ведущие к ним каналы связи защищены криптоалгоритмами, согласно требованиям ГОСТа. Однако слабость такого шифрования заключается в существовании ключа, который хранится на том или ином физическом носителе, например флешке. Завладев им, можно перехватить и расшифровать передаваемую информацию.

Квантовые коммуникации представляют собой технологию обмена данными, которая защищена с использованием квантового распределения ключей шифрования. С помощью устройств, называемых генераторами одиночных фотонов, этим частицам придают особое состояние. Они начинают играть роль элементов хранения и передачи информации. Причем скопировать их состояние, то есть перехватить ключ, хакер не сможет, оставаясь незамеченным.

Фотонами по волоконно-оптической линии связи будет передаваться информация, необходимая для формирования ключей шифрования. Сами же данные перешлют классическим способом.

Одна из проблем заключается в том, что примерно через 140 км фотоны вследствие процессов рассеивания меняют свое состояние. Эту проблему разработчики решают, планируя построить на линии длиной 670 км шесть защищенных промежуточных узлов.

Изготовление оборудования представляет собой отдельную, довольно сложную задачу. Дело в том, что производственных образцов таких систем не существует. Более того, пока в России нет не только предназначенных специально для его сертификации лабораторий, но и нормативов технических заданий, отражающих требования по безопасности. На данный момент лишь одна компания в России изготовила оборудование, создав собственное техническое задание и согласовав его с ФСБ — «ИнфоТеКС».

Технология пригодится сервисам, предоставляющим госуслуги в электронном виде. Огромный объем персональных данных требует соответствующей защиты. По той же причине в качестве потенциальных пользователей выступают банки. Кроме того, квантовые ключи необходимы для защиты информационных систем государственных корпораций — «Росатома», «Ростеха», РЖД и др.

Реализовать проект планируется в 2021 году, но уже к концу 2020 появится прототип данного сервиса. В перспективе квантовую сеть могут продлить до Санкт-Петербурга.

Третий способ предотвращение кибератак - идентификация пользователя.

Только представьте, если бы каждый пользователь имел свою уникальную электронную подпись, и никто не смог бы ее повторить, тогда случаев взломов было бы намного меньше, так же как и утечек информаций.

Электронную цифровую подпись надежно защитят от взлома с помощью новой российской технологии квантового шифрования. Причем «поставить» свою подпись на документе можно будет дистанционно, используя спутник или оптоволокно. В ближайшем будущем квантовые криптографические алгоритмы планируют использовать в автомобильных брелоках, ключах от квартиры и в любых дистанционных системах идентификации «свой-чужой», где особенно важна защита от хакеров.[6]

Электронная цифровая подпись (ЭЦП) — эквивалент обычной, которую мы привыкли ставить от руки. По сути ЭЦП вносит криптографические преобразования в документ, оставляя на нем своеобразный цифровой след владельца. Проблема в том, что в последние десятилетия разные математические группы успешно строят алгоритмы атак на криптографические хеш-функции, лежащие в основе ЭЦП. Именно хеширование преобразует цифровой код документа в строку знаков конкретной длины.

Хеш-функция должна отвечать следующим требованиям. Во-первых, поиск самого ключа по коду подписанного документа должен быть максимально сложным, а в идеальном случае неосуществимым. Во-вторых, появление одинаковых кодов преобразованных документов при разных секретных ключах (это совпадение называется коллизией) должно быть максимально маловероятным.

Теперь при реализации технологии ЭЦП используют квантовую хеш-функцию. Она преобразует исходный ключ в квантовое состояние, то есть в совокупность кубитов — наименьших элементов хранения информации, которые одновременно находятся в состоянии и нуля, и единицы. Согласно законам квантовой механики, из каждого кубита можно извлечь только один бит информации — ноль или единицу.

Если объем кода документа составляет один гигабайт данных, после проставления квантовой цифровой подписи он поместится на 100 кубитах. Однако когда мошенник захочет скопировать данные, он сможет «вытащить» только 100 бит информации, восстановить ключ из которых просто невозможно.

Несмотря на быстрое распространение и высокую угрозу, кибератаки можно предотвратить или успешно пресечь. Если все проекты, которые на данный момент разрабатываются, начнут действовать, то государство сможет усилить защиту от кибератак и уменьшить процент киберпреступности. Но помимо этого, нужна помощь каждого пользователя, ведь многие киберпреступления происходят из-за неосторожности самих пользователей. Проводя дополнительные занятия, распространяя меры предостережения от злоумышленников, также уменьшается шанс кибератак.

Список использованных источников

1. Указ президента российской федерации «Об утверждении доктрины информационной безопасности российской федерации» от 5 декабря 2016 года № 646. Доступ из справочной правовой системы «Консультант плюс»
2. https://chto-eto-takoe.ru/cyberattack (дата обращения 9.02.2019)
3. https://www.kommersant.ru/doc/3957187 (дата обращения 9.02.2019)
4. https://iz.ru/950558/aleksei-ramm-bogdan-stepovoi/komanda-unichtozhit-v-voennykh-okrugakh-poiaviatsia-tcentry-kiberzashchity] (дата обращения 9.02.2019)
5. https://iz.ru/941187/olga-kolentcova/uzly-sviazi-v-rossii-postroiat-pervuiu-kommercheskuiu-kvantovuiu-set] (дата обращения 9.02.2019)
6. https://iz.ru/913105/olga-kolentcova/vydaiushchaia-lichnost-elektronnuiu-podpis-zashchitiat-kvantovym-shifrovaniem (дата обращения 9.02.2019)

СИСТЕМА ИБ

Конюшин Геннадий Геннадьевич, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктор технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Система информационной безопасности для компании – юридического лица включает три группы основных понятий: целостность, доступность и конфиденциальность. Под каждым скрываются концепции с множеством характеристик.

Под **целостностью** понимается устойчивость баз данных, иных информационных массивов к случайному или намеренному разрушению, внесению несанкционированных изменений. Понятие целостности может рассматриваться как:

- **статическое**, выражающееся в неизменности, аутентичности информационных объектов тем объектам, которые создавались по конкретному техническому заданию и содержат объемы информации, необходимые пользователям для основной деятельности, в нужной комплектации и последовательности;
- **динамическое**, подразумевающее корректное выполнение сложных действий или транзакций, не причиняющее вреда сохранности информации.

Для контроля динамической целостности используют специальные технические средства, которые анализируют поток информации, например, финансовые, и выявляют случаи кражи, дублирования, перенаправления, изменения порядка сообщений. Целостность в качестве основной характеристики требуется тогда, когда на основе поступающей или имеющейся информации принимаются решения о совершении действий. Нарушение порядка расположения команд или последовательности действий может нанести большой ущерб в случае описания технологических процессов, программных кодов и в других аналогичных ситуациях.

Доступность – это свойство, которое позволяет осуществлять доступ авторизированных субъектов к данным, представляющим для них интерес, или обмениваться этими данными. Ключевое требование легитимации или авторизации субъектов дает возможность создавать разные уровни доступа. Отказ системы предоставлять информацию становится проблемой для любой организации или групп пользователей. В качестве примера можно привести недоступность сайтов госуслуг в случае системного сбоя, что лишает множество пользователей возможности получить необходимые услуги или сведения.

Конфиденциальность означает свойство информации быть доступной тем пользователям: субъектам и процессам, которым допуск разрешен изначально.

БЕСПЛАТНОЕ АНТИВИРУСНОЕ ПО И ПЛАТНОЕ ПАКЕТНОЕ ПО ОДИНАКОВО ЗАЩИЩАЮТ ОТ ВИРУСОВ

Королева Полина Алексеевна, курсант 1 курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Безопасность представляет собой комплексное понятие, куда входят технические аспекты надежности оборудования, качество питающей сети, уязвимость программного обеспечения и т.д. Данное ложное высказывание поддерживает 83%. Хотя 56% опрошенных при вопросе о различиях качества бесплатного и платного защитного ПО выразили сомнение относительно того, что качество обоих видов защитного ПО сравнимо, большинство участников опроса не смогли в целом назвать разницу. 15% не имели никакого понятия, насколько бесплатные продукты безопасности проигрывают платным в отношении эффективности. Почти 3% опрошенных считают, что разница состоит в нагрузке на систему: бесплатное ПО больше нагружает систему, чем платное.

Большая разница между платным и бесплатным ПО определяется тем, какие технологии безопасности включает в себя это ПО. Бесплатное защитное ПО предоставляет лишь антивирусную защиту. Платное защитное ПО охватывает больше элементов безопасности. Это было известно только 17% участников опроса.

СИСТЕМАТИЗАЦИЯ МЕТОДОЛОГИЧЕСКОЙ БАЗЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Королькова Дарья Антоновна, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Современный мир, с его возрастающей зависимостью от информационных технологий, все больше становиться похожим на огромную паутину, эластичную по количеству используемых устройств и новым технологиям, и в тоже время жесткую к правилам их использования.

Владельцы активов из покон веков пытались защитить свою собственность от посяганий на неё своих врагов. Двадцать первый век не стали исключением. Информация как актив приобрела достаточно большое распространение во всех сферах жизни, что способствовало росту преступлений связанных с хищением, уничтожением информации.

В последние годы, тема информационной безопасности стала достаточно популярной в России, и этому есть несколько объяснений:

1. Рост активности вредоносного программного обеспечения увеличивается в геометрической прогрессии;
2. Постоянное увеличение бюджетов на информационную безопасность;
3. Начало действия штрафных санкций за невыполнение ФЗ РФ от 26 июля 2006 года №152 «О персональных данных».

Множество законов и подзаконных актов, существующих в области информационной безопасности, разные трактовки определений и способов защиты активов способствует тому, что сотрудники, задействованные в организации защиты информации, не знают, на каких аспектах надо сконцентрироваться, чтобы построить хорошо сбалансированную систему защиты информации.

Цель – систематизировать методологическую базу в области информационной безопасности. В качестве важнейших задач следует выделить:

Проведение анализа международных стандартов в области защиты информации, лучших практик по построению системы обеспечения информационной безопасности.

Обобщение мирового практического опыты по построение надежных систем обеспечения информационной безопасности.

Построение единой понятийной методологической базы в области информационной безопасности с использованием системного анализа.

При построении системы защиты информации следует следовать четырём правилам:

При построении системы информационной безопасности, прогнозируйте действия противника.

Реагируйте на возникшие изменения быстро, вносите изменения точечно.

Постоянно проводите разъяснительную работу среди людей, разъясняя им, что вы делаете и главное зачем.

Ничего лишнего, только самое необходимое. Руководствуйтесь здравым смыслом, и только потом лучшими практиками и рекомендациями.

Проведенная систематизация защитных элементов и механизмов, описанных в настоящей дипломной работе, может использоваться в качестве методического руководства при организации системы защиты информации. Она позволяет моделировать систему защиты информации в зависимости от формы субъекта и выбирать элементы для оптимальной системы защиты информации.

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ОЦЕНКИ ВЛИЯНИЯ РАЗЛИЧНЫХ ПРИЗНАКОВ НА РЕЗУЛЬТАТ ЭКСПЕРТИЗЫ

Кручок Елена Андреевна, курсант 4-го курса
Научный руководитель Плотников Герман Геннадьевич, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Все мы живем в веке информационных технологий, где все, казалось бы, создается для удобства человека, однако именно достижения в сфере науки и техники, внедряясь в нашу повседневную жизнь, не только улучшают ее, но и делают нас уязвимыми, как отдельно взятого человека, так и общество в целом. При использовании определенного программного обеспечения, мобильное устройство человека может трансформироваться из незаменимого гаджета в оружие, активно работая против самого владельца. Скомпрометированное мобильное устройство можно отслеживать и использовать для прослушивания телефонных звонков. Объем информации, хранящейся на устройствах, постоянно возрастает. Мобильные телефоны становятся переносными носителями информации, и они отслеживают все действия их владельцев, в них хранятся такие данные как, фотографии, видеофайлы, электронные переписки, информация о звонках и контактах и многое другое.

Наука о восстановлении цифровых доказательств из мобильных телефонов называется цифровой форензикой. Цифровое доказательство включает в себя любые цифровые данные, которые могут быть использованы в качестве доказательств при раскрытии и расследовании преступлений. Выявление в памяти мобильных устройств криминалистически важной, ориентирующей и доказательственной информации, требует от эксперта целенаправленного поиска и изъятия указанных объектов, извлечения из них имеющих значение для уголовного дела информации, их фиксации и анализа. Также многое зависит от возможностей программных и программно-аппаратных комплексов, которые позволяют в минимальные сроки извлечь важную информацию (в том числе удаленную) из памяти мобильных устройств, SD-карт памяти, SIM-карт. Однако, в процессе исследования мобильных устройств, компьютерные эксперты сталкиваются с некоторыми трудностями, так как большое количество используемых мобильных устройств, требуют специальных знаний и навыков при извлечении из них необходимой информации. В некоторых случаях недостаточно быть опытным компьютерным экспертом, при исследовании мобильного устройства могут возникнуть следующие трудности: для скрытия информации о совершенном преступлении, преступники удаляют важную информацию из памяти мобильных устройств, что создает сложность в извлечении удаленных файлов, а именно в их полном восстановлении.

Для получения информации из мобильных телефонов, компьютерный эксперт применяет следующие методы:

1. ручное извлечение данных;
2. извлечение данных на логическом уровне;
3. извлечение данных на физическом уровне;
5. извлечение файловой системы.

Изолировав мобильное устройство от сетей, компьютерный эксперт приступает к извлечению данных и их анализу, при помощи избранного программного или программно-аппаратного комплекса. Важно отметить, что внешние носители информации (карты памяти) нужно исследовать отдельно, так как возможно внести изменения в данные, хранящиеся на ней, во время исследования мобильного устройства.

Ручное извлечение данных. Данный уровень подразумевает обеспечение доступа к компьютерной информации, имеющейся в памяти мобильного устройства, посредством его клавиатуры или сенсорного экрана. Обнаруженная в ходе исследования информация документируется путем фотосъемки экрана телефона или планшета. Данные метод является

наиболее простым и подходит для любого устройства. Важно отметить, что на данном уровне невозможно получить все данные, а также произвести восстановление удаленных файлов и записей. Несмотря на кажущуюся простоту данного метода, некоторые типы данных возможно получить только данным способом.

Извлечение данных на логическом уровне. Логический метод представляет собой извлечение тех данных, которые хранятся в устройстве и доступны для пользователя, операционная система мобильного устройства телефона позволяет извлекать информацию через API или интерфейс программирования приложений. Данный уровень подразумевает подключение мобильного устройства к рабочей станции эксперта посредством USB-кабеляции «Bluetooth». После этого производится копирование файлов и каталогов, находящихся на логических дисках мобильного устройства. При этом используется интерфейс прикладного программирования, разработанный производителем и предназначенный для синхронизации телефона или планшета с персональным компьютером. Тем не менее, данный уровень извлечения данных также обеспечивает ограниченный доступ к информации, и не позволяет восстановить удаленные данные. Исключением могут служить удаленные записи из баз данных SQLite, использование которых характерно для операционных систем Android. Стертые записи в указанных базах данных не перезаписываются сразу, а помечаются как «удаленные» до тех пор, пока место, занимаемое ими, не понадобится для записи новых данных.

Извлечение файловой системы. Основное различие между логическим извлечением и извлечением файловой системы заключается в том, что криминалистические инструменты могут напрямую обращаться к файлам во внутренней памяти мобильного устройства вместо необходимости обмениваться данными через API для каждого типа данных. Этот прямой доступ позволяет инструментам компьютерной экспертизы извлекать все файлы, присутствующие во внутренней памяти, включая файлы базы данных, системные файлы и журналы. Извлечения файловой системы полезны для изучения структуры файлов, истории просмотра веб-страниц и истории использования приложений на мобильном устройстве. Наиболее важной частью извлечения файловой системы является полный доступ к файлам базы данных на мобильном устройстве. Многочисленные приложения, такие как «iMessage», «SMS», «MMS», «Календарь» и другие, хранят свою информацию в файлах базы данных. Когда пользователь удаляет данные, которые являются частью базы данных, например, SMS, запись в этой базе данных помечается как удаленная и больше не видна пользователю. Эти удаленные данные остаются неизменными в базе данных и подлежат восстановлению, пока база данных не выполнит плановое обслуживание и не будет очищена. Как только этот процесс происходит, данные больше не восстанавливаются.

Извлечение данных на физическом уровне. Этот уровень подразумевает получение побитовой копии всей внутренней памяти мобильного устройства, что позволяет, в том числе, восстановить удаленные записи и файлы. Для извлечения используется API загрузчика (на стадии включения мобильного телефона). Несмотря на привлекательность данного метода, осуществить извлечение данных на этом уровне представляется возможным далеко не всегда: производители зачастую ограничивают возможность чтения внутренней памяти мобильного устройства в целях обеспечения максимальной безопасности. Чтобы обойти данные ограничения, разработчики программного обеспечения для криминалистического исследования мобильных устройств создают собственные загрузчики, которые позволяют не только получить доступ к внутренней памяти, но и, иногда, обойти пароли, установленные пользователями. Из устройства извлекается полная копия памяти. Извлекаются следующие данные: «веб соединения», «журнал событий», «лог-файлы», «медиа», «облачные учётные записи», «органайзер (заметки, календарь)», «пароли», «сообщения», «телефонная книга», «данные приложений», «исполняемые файлы приложений», «удаленные файлы» и т.д.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ЛИЧНОСТИ, ОБЩЕСТВА И ГОСУДАРСТВА ПРИ ПРИМЕНЕНИИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Крылова Светлана Валерьевна, 4 курс
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Информационно-цифровые технологии радикально меняют жизнь человечества и отдельно взятого человека и создают немало социальных проблем, как для общества, так и государства. Современный мир уже невозможно представить без существования информационно-цифровых технологий.

Безусловно, резкий переход и массовое использование информационно-цифровых технологий порождает целое множество угроз безопасности Российской Федерации. Поэтому государственный информационный суверенитет и информационная безопасность защищаются дополнением пункта «м» статьи 71 Конституции Российской Федерации. В частности, в введенном пункте находятся «обеспечение безопасности личности, общества и государства при применении информационных технологий; оборот цифровых данных». Поправки в Конституцию РФ от 04.07.2020 г. направлены на создание условий обеспечения всех видов государственной безопасности, в том числе связанных с обеспечением безопасности граждан, общества и государства от рисков, вызванных информационными технологиями и оборотом цифровых данных. Внесенные изменения в Конституцию РФ в настоящее время стали необходимыми, неизбежными и целесообразными, которые встретили сопротивление со стороны некоторых консервативных кругов общества и граждан. Неустойчивость конституции, внесение в них изменений или полный пересмотр характерны для ситуаций изменения в стране общественно-политического и экономического положения и поэтому в Конституции РФ необходимо выразить политическую платформу посредством внесения в нее изменений и, особенно, в обеспечении безопасности граждан, общества и государства. На сегодняшний день информационные технологии, а именно киберпреступность по праву можно назвать серьезной проблемой 21 века. Мир все больше осознает опасность информационных технологий, а именно повышенная зависимость от цифровой инфраструктуры, которая стала основным каналом эффективного взаимодействия во всем мире, главным способом нашей жизнедеятельности в общении, работе и поддержке друг друга и приводит к рискованным последствиям.

Мошенничество, перехват чужой информации, вмешательство в чужую компьютерную систему, повреждение, уничтожение или изменения ее работы стало королем криминала в современном мире цифровых и информационных технологий. Перечислить все возможные варианты информационных правонарушений и преступлений просто невозможно.

Всеобщая цифровизация и информационные технологии обнаружили уязвимые точки, связанные с безопасностью граждан и государства. И поэтому в наше время особое внимание уделяется проблемам, связанными со стремительным развитием современного общества, которое порождает множество угроз, в том числе природного, техногенного, информационного, экологического и иного характера, а также в части распространения терроризма и экстремизма киберпреступности, как внутри страны, так и на международном уровне, проблемы с транспортной безопасностью и управленческих рисков. В этот перечень также входят угрозы информационной безопасности, занимающие не менее важное место и требующие особого внимания и комплексного подхода к их разрешению. К ним относятся:

– вывод из строя информационного обеспечения деятельности органов государственной и исполнительной власти и муниципальных служб;

– перехват трансляций систем оповещения и информирования населения;

– доступ злоумышленников к информации, которая включает в себя сведения о деятельности органов государственной власти;

– несанкционированный доступ к управлению информационными ресурсами, что может привести к необратимым последствиям;

– оказание посредством средств массовой информации и сети Интернет информационного воздействия на население, с целью вызова негативных эмоций и изменения мышления в выгодную для злоумышленника сторону (манипулирование массовым сознанием с использованием информационно-психологического воздействия);

– неполная реализация прав граждан в области получения и обмена достоверной информацией, что также приводит к манипулированию массовым сознанием;

– деятельность отдельных СМИ, блогов и иных источников сети Интернет узкой направленности, может провоцировать появление социальной, межнациональной и религиозной напряженности, что приведет к реальным столкновениям противоборствующих сторон, созданных данными организациями;

– распространенные махинации в финансовой сфере, связанные с проникновением в компьютерные системы и сети, что представляет собой большую угрозу как для отдельных пользователей, так и для государства в целом.

Такие угрозы и риски ставят вопрос о применении в отношении населения мер по повышению уровня общественной безопасности и правопорядка, для чего требуется улучшить координацию деятельности органов государственной власти и служб, в ведении которых находится решение данных задач. При улучшении работы деятельности данных органов есть возможность предотвратить на начальном уровне возникающие правонарушения, представляющие угрозу в направлении информационной безопасности.

Подход к решению данных задач должен быть комплексным и многосторонним, включающим использование информационных систем мониторинга, прогнозирования предупреждения и ликвидации возможных угроз. Ни для кого не секрет, что внедрение технологий - это, безусловно, важный, но к тому же ответственный шаг. Помимо упрощения контроля и устранения последствий чрезвычайных ситуаций и правонарушений с интеграцией под ее управлением действий информационно-управляющих подсистем дежурных, диспетчерских, муниципальных служб для их оперативного взаимодействия в интересах муниципального образования, они требуют качественного администрирования и постоянного обновления, дабы избежать несанкционированного доступа со стороны злоумышленников. Внедрение информационных технологий в правоохранительную деятельность в первую очередь обусловлено распространением преступлений в информационной сфере. Применение злоумышленниками современных технологий требует соответствующих подходов к пресечению их противоправных действий. Поэтому расследование цифровых следов при совершении преступлений с использованием информационных технологий возможно только при использовании правоохранительными органами аналогичных информационных средств и технологий, желательно являющихся перспективнее и новее, чем у противника, что сложно контролировать при скорости развития современных сетей и средств.

Необходимость развития и внедрения информационных технологий связана со скоростью принятия решений. В условиях динамичной экономики, деятельности всей человеческой деятельности, основанной на информационных технологиях, в критических ситуациях необходимо принимать грамотные управленческие решения в кратчайшие сроки. Развитие автоматизированных систем, банков данных, систем анализа и оповещения позитивно влияет на принятие выверенных решений, которые требуют мгновенного получения и анализа всей информации.

К названным причинам внедрения информационных технологий следует добавить экономическую целесообразность, необходимость сокращения административного аппарата, более качественного предоставления государственных услуг, повышения качества и уровня жизни.

Таким образом, все вышеперечисленные причины по внедрению современных технологий ставят перед правоохранительными органами и органами государственной власти такие задачи, как создание коммуникационной платформы, основой которой является устранение угроз общественного правопорядка и общественной безопасности путем установления межведомственного взаимодействия. Для этого важно уяснить возможные точки уязвимости, своевременно и быстро реагировать на возникающие проблемы, связанные с возникающими чрезвычайными ситуациями, также и в области информационной безопасности.

В соответствии с Федеральным законом от 5 мая 2014 года №97-ФЗ «О внесении изменений в Федеральной закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» организаторы рассылки информации в сети Интернет на сегодняшний день в течении шести месяцев должны передавать информацию о случаях приема, передачи, обработки голосовой информации, текстовых сообщений, изображений, видео и иных сообщений пользователей, государственным органам, которые осуществляют оперативно-розыскную деятельность или обеспечивают безопасность Российской Федерации. Для гарантированного получения данной информации в Федеральный закон от 12.08.1995 №144 «Об оперативно-розыскной деятельности» внесли еще одно оперативно-розыскное мероприятие – получение компьютерной информации.

В сфере правоохранительной деятельности интенсивно развиваются системы информационного управления, системы обработки и идентификации дактилоскопической, генной, баллистической и иной криминалистически значимой информации, программное и информационное обеспечение перспективных и современных автоматизированных систем управления, информационно-справочную работу для подразделений МВД России.

Между тем, действующими эффективными технологиями на сегодняшний день, которые позволяют в большей мере обеспечивать общественную безопасность, следует назвать видеонаблюдение и видеофиксацию. Также существуют различные методы получения информации с видео, в их числе: возможность снятия видеопотока с камер видеонаблюдения о правонарушениях и ситуациях чрезвычайного характера, получение информации о повреждениях различных объектов коммуникаций, любого вида имущества, если есть возможность и средства для получения такой информации. Для этого проводится анализ видео- и аудиопотоков, посредством регистрации событий, происходящей автоматически, анализа видеопотока в реальном времени, поиск, распознавание и идентификация лиц, присутствующих в данном видеоролике и совершающего противоправные действия.

Применение технических средств на современном этапе их развития позволяет раскрывать не только преступления в информационной сфере, которых с каждым днем становится все больше и приобретающих все более изощренные формы применительно достижений науки и техники, но и бытовые и часто встречающиеся в реальной жизни, за пределами информационных сетей, правонарушения и преступления оперативней раскрываются за счет применения компьютерных систем и сетей сотрудниками правоохранительных органов. Сейчас сложно представить работу даже обычного участкового уполномоченного полиции без компьютерных технологий, автоматизированных систем, представляющих в удобной и наглядной форме упорядоченные сведения обо всем, что происходит на его участке. Поэтому, неудивительно, что для оперативных сотрудников наличие современных средств связи и коммуникаций, а также умение ими пользоваться является неотъемлемой частью их деятельности и важной особенностью работы. Не зря в правоохранительных органах есть специальные подразделения, деятельность которых направлена на применение, тестирование и внедрение информационных технологий в деятельность сотрудников для оптимизации службы и повышения раскрываемости дел.

Современные технологии расширили перечень предметов и документов – вещественных доказательств, подлежащих оперативно-розыскной и криминалистической регистрации. Регистрация и долговременное хранение интернет-трафика, всех телефонных соединений, наличие жесткой взаимосвязи абонента и базовой станции, а также технические возможности современных компьютерных средств и систем управления базами данных позволяют оперативно обработать колоссальные объемы информации и получить сведения, которые облегчают расследование и раскрытие преступлений. Современные информационные технологии и автоматизированные базы данных помогают сотрудниками оперативно найти и изучить личности всех субъектов преступной деятельности, быстро проверить все возможные и выдвигаемые версии, принять законное решение и оценить его в возможно короткие сроки.

Развитие информационно-телекоммуникационных технологий (ИТС) имеет большое значение для обеспечения безопасности личности, общества и государства. В современном информационном пространстве при увеличении различных угроз, в числе которых и информационные, разнообразии форм компьютерных преступлений, распространенное применение искусственного интеллекта, присутствие и возможность использования информационно-телекоммуникационных технологий во всех сферах правоохранительной, экономической, регулятивной деятельности является необходимым и весьма перспективным направлением деятельности для обеспечения безопасности личности, общества и государства. Основным требованием для обеспечения эффективного и незамедлительного взаимодействия служб, отвечающих за общественную безопасность и правопорядок необходимо создание единой информационной среды и ее постоянное обновление и качественное профессиональное администрирование. Продолжать развитие интегрированных банков данных значимой оперативно-розыскной и криминалистической информации для достижения более высокого уровня информатизации органов исполнительной власти, в частности органов внутренних дел. Уровень технической оснащенности всех органов оперативно-розыскной деятельности телекоммуникационной инфраструктурой и информационными ресурсами должна соответствовать современным вызовам и техническим требованиям.

В сложившихся требованиях информационных правоотношений нужно учитывать существующие информационные угрозы и риски, обеспечивать конституционные гарантии права личности на частную жизнь, безопасность общества и государства от преступных посягательств.

Таким образом можно сделать вывод, что соблюдение и защита прав и свобод человека и гражданина важный признак правового государства.

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ПРОИЗВОДСТВЕ

Кузнецов Матвей Николаевич, командир отделения, сержант полиции
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Компьютерные вирусы. Анализ их работы и возможные последствия

Вирус – главный враг компьютера, ведь он способен замедлить или полностью уничтожить работоспособность компьютера, а что ещё хуже, злоумышленники с помощью вирусов способны взламывать сети, красть важную информацию и даже дистанционно управлять чужим персональным компьютером.

В настоящее время проблема вирусов и их возможных последствий очень актуальна, ведь с каждым днем вирусов становится всё больше, а последствия, к которым они могут привести опаснее. Когда вирусы впервые появились, никто и не мог предположить, к какой глобальной проблеме это может привести, ведь в наше время компьютеры используются абсолютно везде, по этому, к сожалению, начали появляться программы-вирусы.

Во многих странах были приняты законы о борьбе с компьютерными преступлениями. Немало сил было приложено на разработку специальных программ для защиты персонального компьютера (ПК) от вирусов, что требует от пользователя ПК знаний о природе вирусов.

Вирус – это вредоносное программное обеспечение, которое внедряется в код программ, системные области памяти и распространяет свои копии по разнообразным каналам связи. Его основной целью является распространение.

Вирусы распространяются с помощью программного обеспечения и заменяются другими программами, регистрация в автозагрузке осуществляется через реестр и многое другое. Вирусом или его носителем могут быть не только программы или машинный код, но также любая информация, доступная для автоматически выполняемых команд, например, пакетные файлы и документы Microsoft Word и Excel, доступные макросы. Кроме того, вирус может использовать уязвимости в популярном программном обеспечении (например, AdobeFlash, InternetExplorer, Outlook) для проникновения на компьютер, для которого его данные распространяются в обычных данных (изображения, тексты и т.д.) Наряду с эксплойтом, который эксплуатирует уязвимость.

После того, как вирус успешно введен в код программы, файл или документ перейдет в спящий режим. Чтобы запустить компьютерную программу, нужно запустить зараженную программу. Это означает, что вирус может оставаться неактивным на компьютере без каких-либо признаков повреждения. Однако вирус может начать действовать. В зависимости от целей, вирусное программирование приводит к разрушительным последствиям, таким как конфиденциальные информационные данные.

Есть несколько способов распространения компьютерных вирусов:

1. Дискеты. Самый распространенный канал заражения в 1980-1990-е гг. В настоящее время практически отсутствует из-за появления более распространенных и эффективных каналов и отсутствия флоппи-дисководов во многих современных компьютерах.
2. Флеш-накопители(флешки). В настоящее время USB-флешкизаменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, а с 2000-х годов всё большую роль играют мобильные телефоны, особенно смартфоны (появились мобильные вирусы).
3. Электронная почта.Обычновирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты. В некоторых

письмах могут содержаться действительно только ссылки, то есть в самих письмах может и не быть вредоносного кода, но если открыть такую ссылку, то можно попасть на специально созданный веб-сайт, содержащий вирусный код.

4. Системы обмена мгновенными сообщениями. Здесь также распространена рассылка ссылок на якобыфото, музыку либо программы, в действительностиявляющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

5. Веб-страницы. Возможно также заражение через страницы Интернета ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов[4], ActiveX-компонент. В этом случае используются уязвимости программного обеспечения, установленного на компьютере пользователя, либо уязвимости вПОвладельца сайта (что опаснее, так как заражению подвергаются добропорядочные сайты с большим потоком посетителей), а ничего не подозревающие пользователи, зайдя на такой сайт, рискуют заразить свой компьютер.

6. Интернет и локальные сети(черви).Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер. Уязвимости — это ошибки и недоработки в программном обеспечении, которые позволяют удаленно загрузить и выполнить машинный код, в результате чего вирус-червь попадает в операционную систему и, как правило, начинает действия по заражению других компьютеров через локальную сеть или Интернет. Злоумышленники используют заражённые компьютеры пользователей для рассылки спама или для DDoS-атак.

Как видно, способов распространения компьютерных вирусов немало. Для предотвращения заражения необходимо соблюдать элементарные меры предосторожности:

1. стараться использовать только проверенные ресурсы в сети Интернет;
2. не скачивать сомнительные программы, а также не нажимать на сомнительные картинки;
3. при получении писем от неизвестного адресата, обращать внимание на расширение приложенных файлов. Если они имеют такие типы как:*.bat,*.vbs,*.scr,*.exe, то не стоит скачивать эти приложения, они могут быть заражены или попросту являются вирусом трояном;
4. применять лицензионные антивирусы.

Как известно, на данный момент по всему миру разработаны десятки тысяч вирусов и каждый из них работает по определенной схеме. Поэтому можно объединить работу всех вирусов и выявить три основных этапа:

1. Заражение
2. Размножение
3. Атака

Но, стоит отметить, что есть вирусы типа “Бомба”, которые способны обойтись без размножения. Также есть вирусы “троянский конь”, которые способны обойтись без атаки, а есть вирусы, которые имеют этап маскировки, получившие название стелс-вирусов или “полиморфные”

Разберем три основные этапа более подробно:

Заражение. На этом этапе вирус внедряется в код компьютера, затем на файлы через внешний носитель. Обычно такое происходит при запуске уже зараженной программы. В память компьютера записывается код вируса, а затем оттуда копируется на внешние устройства (жесткий диск и т.д.)

Размножение. Это серия последовательных заражений файлов. При запуске такого зараженного файла код вредоностной программы начинает перемещаться в оперативную память, а затем она становится резидентной на время работы компьютера. Чем больше файлов запускается, тем больше заражение.

Атака. На этой фазе происходят разрушения. Обычно вирусы не начинают атаку до того, как размножаться, т.к. в таком случае их легко уничтожить. Поэтому перед атакой

вирус должен сделать несколько своих копий и уже после этого начать атаку. Некоторые вирусы запрограммированы так, что они работают по “счетчику”, то есть до момента, пока не будет сделано определенное количествой своих копий, другие вирусы запрограммированы так, что они не начнут атаку без команды из удаленного центра, а третьи запускаются всего лишь при открытии определенных файлов или документов.

К признакам появления вируса можно отнести:

- замедление работы компьютера;
- невозможность загрузки операционной системы;
- частые "зависания" и сбои в работе компьютера;
- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- увеличение количества файлов на диске;
- изменение размеров файлов;
- периодическое появление на экране монитора неуместных системных сообщений;
- уменьшение объема свободной оперативной памяти;
- заметное возрастание времени доступа к жёсткому диску;
- изменение даты и времени создания файлов;
- разрушение файловой структуры (исчезновение файлов, искажение каталогов и др.);
- загорание сигнальной лампочки дисковода, когда к нему нет обращения;
- вывод на экран непредусмотренных сообщений или изображений;
- диски или дисководы недоступны;
- печать выполняется с ошибками;
- открываются искаженные меню и диалоговые окна.

Компьютерные вирусы во всем мире наносят громадный ущерб. Эти маленькие вредоносные программы живут по трём правилам – Размножаться, Скрываться и Портить. И какие потрясения бывают, когда однажды пропадают данные, которые собирались и накапливались может ни один год....

Чтобы этого не произошло, нужно знать о существовании компьютерных вирусов и уметь защищать свои данные.

ЕСЛИ НЕ ОТКРЫВАТЬ ЗАРАЖЕННЫЕ ФАЙЛЫ, ТО ПК НЕЛЬЗЯ ЗАРАЗИТЬ

Кузнецов Владимир Романович, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Если не открывать зараженные файлы, то ПК нельзя заразить.

Это высказывание, как и некоторые другие, основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний, и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно лишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открывания зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

Большинство вредоносных программ распространяется через USB-накопители (12,83%).

Ради справедливости отметим, что в последние годы популярность "флешек" и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. "Поэтому настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом, можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя", - пишут исследователи из G Data.

Я не посещаю странные веб-сайты, поэтому мне не угрожает заражение при "попутной загрузке" (13%).

Данное утверждение можно опровергнуть так же, как и шестой тезис ("Риск встретить вредоносное ПО на порносайтах выше, чем, например, при посещении сайтов о конном спорте или о путешествиях"). Тематика веб-сайта не играет для кибер-преступников никакой роли. Они заинтересованы в том, чтобы с минимальными затратами заразить вредоносными кодами максимальное количество посетителей. Это удается злоумышленникам, помимо всего прочего, с помощью манипуляций с баннерами и постоянных атак крупных доменов. В случае успеха и получения доступа они внедряют вредоносный код с помощью т.н. эксплойт-инструментов, и специальные знания для этого не требуются. Веб-сайты, которые на протяжение многих лет считались достойными доверия, могут очень быть взломанными и в результате таить в себе опасность заражения. Однако данный тезис считают правдивым всего лишь 13% опрошенных.

ПРИМЕНЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Кунин Иван Андреевич, командир отделения
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Актуальность темы заключается в том, что на сегодняшний момент необходимы качественные и надежные средства защиты, позволяющие смело хранить разного количества объема личных данных, сбережений на собственном виртуальном аккаунте, при этом не беспокоясь за их конфиденциальность и сохранность.

Главная тенденция развития современного общества тесно связана с ростом информационной безопасности (ИБ). Приоритетными на современном этапе рассматриваются вопросы ИБ.

Современные технологии постоянно совершенствуются, поэтому такими основами жизни, как безопасность, не следует пренебрегать.

Известно, что более 25 % злоупотреблений информацией в информационных системах (ИС) совершаются внутренними партнерами, пользователями и поставщиками услуг, обладающими доступом к информационным системам. 64% из них – это кража информации, а 21% - финансовое мошенничество. Все это становится возможным из-за несовершенства технологий аутентификации пользователей ИС и разграничения доступа. Одним из приоритетов развития информационных систем является совершенствование управления доступом и регистрация пользователей.

В настоящее время информационные технологии (ИТ) имеют важнейшее значение во многих сферах деятельности. Все труднее становится представить обычный рабочий день без взаимодействия с интернетом. ИТ стали неотъемлемой частью государственного управления, бизнеса, развлечений и т.д. Появляется огромное количество ресурсов, соответственно, требующие необходимую защиту личных данных. В связи с достижением такого результата, что логично, возникают неприятели, которые не прочь нажиться на халатности, ошибках и слабостях владельцев аккаунтов информационных устройств. А для того, чтобы предотвратить мошеннические действия нужна защита, с помощью которой можно будет пресечь утечку информации.

На данный момент в автоматизированных системах присутствует разнообразие средств и методов защиты информации, что наглядно отражает многообразие возможных способов несанкционированных действий.

Аутентификация и является собой прекрасный пример создания механизма защиты личных данных. Она представляет собой процедуру установления подлинности или соответствия.

Многофакторная аутентификация, как ее по-другому называют, - это два уровня защиты. Как часто бывает, первый уровень – логин и пароль. В качестве второго уровня выступают различные средства защиты:

- Одноразовые пароли (почта или SMS) - это проверочный код, необходимый для подтверждения подлинности.
- Телефонный звонок.
- Токены - компактное устройство, предназначенное для обеспечения информационной безопасности пользователя.
- Биометрические данные - сравнение и обзор методов проверки.
- Приложения-аутентификаторы.

- Резервные ключи.

Использование той или иной формы двухфакторной аутентификации значительно затрудняет злоумышленникам взлом учетной записи, обеспечивая безопасность компании и данных клиентов.

Необходимость применения данного способа защиты пользователей от несанкционированного доступа возникла у многих сайтов и ресурсов глобальной сети интернет. Вот, например, небольшой перечень порталов для которых это не просто атрибут в настройках, а некоторый ключевой элемент, который может в существенной степени повлиять на безопасность учетной записи: «Яндекс», «ВКонтакте», «Facebook», «Google», «Twitter», «Instagram».

Сейчас у каждой уважаемой себя компании или организации, которая осуществляется деятельность во всемирной паутине и, где есть возможность регистрировать аккаунт - должна быть функция двухфакторной аутентификации. Здесь даже дело не в уважении, а в требовании к безопасности в современном мире. Пароль и ПИН-код при наличии времени и ресурсов подбирается за крайне малый промежуток времени, в то время, как получить второй фактор не всегда представляется возможным для преступника. Именно, поэтому наличие данной функции можно наблюдать практически на каждом сервисе или сайте (где есть учетные записи пользователей.

В данной теме было рассмотрено применение двухэтапной аутентификации. Это является еще одним плюсом при оценивании его полезности, так как в случае отсутствия интернета можно воспользоваться способом, не требующим подключения интернет соединения.

Подводя итог, можно сказать, что двухфакторная аутентификация стала практически необходимой частью процесса входа в аккаунт. Именно этот способ добавил уверенности не возникновения утечки личных данных, а также надежности его применения.

Также необходимо заметить присутствие настоящего метода аутентификации на большом количестве известных ресурсах страны.

Двухфакторная аутентификация обладает, хоть и в маленькой степени, уязвимостями, но при умелом и качественном подходе к защите собственных данных этого можно избежать.

Данный способ не обязательно активировать повсеместно, где только заблагорассудится. Достаточно лишь защитить аккаунты, в которых хранятся конфиденциальная информация, денежные средства и пароли.

Список использованных источников

1. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности / Родичев Ю.А. – М.: Питер, 2017. – 550 с.
2. Шелупанова, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / Шелупанова А.А., Груздева С.Л., Нахаева Ю.С. – М.: Горячая линия-Телеком, 2015. – 256 с.
3. Головко, Н. Системы и методы аутентификации пользователей [Электронный ресурс]. / Н. Головко. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods#part3
4. Двухфакторная аутентификация [Электронный ресурс]. / – Режим доступа: http://withsecurity.ru/chto-takoe-dvuhfaktornaya-autentifikaciya
5. Донохью Б. Двухфакторная аутентификация: что это и зачем оно нужно? [Электронный ресурс]. / Б. Донохью. – Режим доступа: https://www.kaspersky.ru/blog/2fa-practical-guide/21495/
6. Козориз, А. 5 способов двухфакторной аутентификации, их преимущества и недостатки [Электронный ресурс]. / А. Козориз. – Режим доступа: https://lifehacker.ru/two-factor-authentication/

КЛЮЧЕВЫЕ НАПРАВЛЕНИЯ В РАЗВИТИИ ИНФОРМАЦИОННЫХ СИСТЕМ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Курбатова Мария Сергеевна, курсант 4-го курса
Научный руководитель Орехов Павел Васильевич, старший преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В настоящее время применение информационных технологий играет ключевую роль в расследовании, раскрытии и пресечении правонарушений и преступлений. Стоит отметить, что благодаря использованию информационных технологий возрастает и быстрота принятия решений при выполнении сложных оперативных задач. Также оптимизируется и работа иных подразделений органов внутренних дел, к примеру, подразделений управления и обеспечения, что помогает решать личные вопросы сотрудников более быстро и эффективно. В ст.11 Федерального закона РФ «О полиции» закрепляется обязанность использования достижений современной науки и техники в деятельности органов внутренних дел [1].

На сегодняшний день в органах внутренних дел РФ происходит построение комплексной информационной системы, а также объединение уже имеющихся данных в единый цифровой формат.

Дальнейшее развитие информационных технологий в ОВД можно разделить на следующие направления:

1. создание новейших информационных ресурсов для работы с данными, а также совершенствование и упрощение использования уже имеющихся информационных систем. Использование технологии «Big data» позволяет работать с большим объемом данных, тем самым способствуя раскрытию преступлений в экономической сфере (отслеживание банковских операций и переводов), предупреждение дорожно-транспортных преступлений (использование данных о GPS-сигнале автомобиля), преступлений в сфере компьютерной информации (получение данных о пользователе, его местоположении и взаимодействии с другими лицами) [2].

2. перевод документов из бумажной формы в цифровую. Изначально сложность использования электронных документов выражалась в отсутствии юридической силы документа, его подлинности и целостности. В настоящее время использование электронной подписи позволяет решить данную проблему, так как документы, подписанные электронной подписью, имеют равную юридическую силу с документом, подписанным обычной подписью. Электронная подпись позволяет также гарантировать подлинность документа [3]. Использование системы электронного документооборота позволяет сократить количество служб, занятых работой с документами, упрощает работу с документами, помогает осуществлять контроль за исполнением документов;

3. развитие ведомственной технологической инфраструктуры. К примеру, с помощью системы передачи данных по защищенному каналу связи «Барс», сотрудники правоохранительных органов могут в кратчайшие сроки получить информацию о гражданах, автомобилях, а также информацию из базы данных о разыскиваемых лицах. В ИЦ применяются программно-технические комплексы ИБД-Регион, позволяющие обеспечить доступ сотрудникам ОВД к базам данных содержащим оперативно-справочную информацию, розыскную и криминалистическую [4].

4. расширение межведомственного взаимодействия;

5. организация и контроль за обеспечением соблюдения режима секретности и защиты персональных данных лиц.

В заключение стоит отметить, что единая система информационно-аналитического обеспечения деятельности МВД (ИСОД) позволяет организовать системный подход к использованию и внедрению автоматизированных систем. Однако, совершенствование уже имеющихся систем и внедрение новых позволит сократить время раскрытия преступлений

сотрудниками правоохранительных органов, повысить защищенность всей системы и объединить данные между ведомствами в единый информационный ресурс.

Список использованных источников

1. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 13.07.2015, с изм. от 14.12.2015) «О полиции» // Собрание законодательства РФ. – 14.02.2011. – № 7. – ст. 900.

2. Измалкова С.А. Использование глобальных систем «Big data» в управлении экономическими системами / С.А. Измалкова, Т.А.Головина // Известия Тульского государственного университета. Экономические и юридические науки. – 2015. – №4. – С.151–158.

3. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 23.06.2016, с изм. от 31.12.2017) «Об электронной подписи».

4. Авдеева Е.В. Оптимизация деятельности правоохранительных органов в контексте внедрения информационно-коммуникационных технологий / Е.В. Авдеева, В.А.Гордей // Закон и право. – 2018. – №10. – С.93-95.

ИНФОРМАЦИОННО - ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ, КАК ИНСТРУМЕНТ ВЕДЕНИЯ ИНФОРМАЦИОННОГО ПРОТИВОБОРСТВА

Иванов Андрей Андреевич, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В настоящее время очень актуальна тема информационного противоборства, или информационной войны. Информационно-телекоммуникационные технологии занимают в данном процессе значительную, так как являются инструментом создания и распространения информации.

Необходимо рассмотреть ряд понятий.

Информация – это сведения (сообщения, данные) независимо от формы их представления.

Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информационно-телекоммуникационная сеть - технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.

Информационное противоборство – это противоборство с использованием всего спектра информационных возможностей, осуществляемое в целях достижения информационного превосходства над противником.

Информационное противоборство в настоящее время ведется весьма активно. Это можно увидеть по политическим отношениям как внутри страны, где, как пример можно привести протестные акции Навального, так и за пределами Российской Федерации, что можно видеть в отношениях между Россией и США. И в том и в другом случае используются методы информационного противоборства. Война внутренняя и внешняя сейчас ведется не с помощью ядерного оружия. Она ведется с помощью искажения информации, преподносимой людям различных стран для формирования в их сознании определенного мировосприятия.

Что бы раскрыть вышенаписанное необходимо рассмотреть три свойства информации.

Первое сущностное свойство информации – **реакция**. Это свойство информации легко раскрыть на примере общения. Если человек реагирует, принимает участие в дискуссии – он воспринимает информацию, если не реагирует – то не воспринимает.

Реактивная информация возникает как реакция человека на внешние воздействия и внутренние побуждения. Она возникает в мозгу человека как некая интерпретация полученных сообщений. Или не возникает, если вам это неинтересно.

Второе сущностное свойство информации – **ресурсность**. Есть биологическая ресурсная информация, которая передается через генетический код. На ней построена вся эволюция. А есть социальная ресурсная информация. Это все, что создано человеком: нарисовано, написано, построено. Внешние носители постоянно совершенствуются – от папируса до цифровых носителей сейчас. То есть, если говорить простыми словами, ресурсная информация, это все те знания, которые человек накапливает на различных носителях.

Третье, самое фундаментальное – свойство информации – способность отражать окружающую реальность. Это **фоновая информация**. Это информация об окружающем человека мире.

Все три составляющие неразрывно связаны между собой и позволяют воздействовать на человеческое сознание.

Роль информационно-телекоммуникационных технологий я данном процессе заключается в том, что они, как бы являясь инструментом формирования информационного воздействия.

Ведь в настоящее время технические возможности создания и распространения информации не ограничены благодаря крупнейшей информационно-телекоммуникационной сети интернет. С ее помощью и ведется большинство информационных противодействий.

Информационно-телекоммуникационные технологии дают огромные возможности для ведения «информационных войн». Он написания и печати различных плакатов до монтажа видеофайлов. Все эти способы создания и распространения ложной, или «фейковой» информации позволяют формировать у людей определенные настроения и направлять их действия в нужное русло. Это является, своего рода, преобразованием информации в энергию действий и поступков. И что бы этому противодействовать, необходимо найти рычаги воздействия на этапах формирования позиции людей во избежание различных последствий информационного воздействия в виде различных акций или даже войны.

МЕТОДЫ И СРЕДСТВА ОБХОДА АНТИВИРУСНЫХ СИСТЕМ, СРЕДСТВ СЕТЕВОЙ ЗАЩИТЫ, СРЕДСТВ ЗАЩИТЫ ОС

Лащёнов Павел Михайлович, курсант 2-го курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Средства защиты информации — это совокупность инженерно-технических, электрических, электронных, оптических и других устройств и приспособлений, приборов и технических систем, а также иных вещных элементов, используемых для решения различных задач по защите информации, в том числе предупреждения утечки и обеспечения безопасности защищаемой информации.

В целом средства обеспечения защиты информации в части предотвращения преднамеренных действий в зависимости от способа реализации можно разделить на группы:

1) Технические (аппаратные) средства. Это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, сторожа, защитная сигнализация и др. Вторую — генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества технических средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны — недостаточная гибкость, относительно большие объем и масса, высокая стоимость;

2) Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Преимущества программных средств — универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. Недостатки — ограниченная функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокая чувствительность к случайным или преднамеренным изменениям, возможная зависимость от типов компьютеров (их аппаратных средств);

3) Смешанные аппаратно-программные средства реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства;

4) Организационные средства складываются из организационно-технических (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых (национальные законодательства и правила работы, устанавливаемые руководством конкретного предприятия). Преимущества организационных средств состоят в том, что они позволяют решать множество разнородных проблем, просты в реализации, быстро реагируют на нежелательные действия в сети, имеют неограниченные возможности модификации и развития. Недостатки — высокая зависимость от субъективных факторов, в том числе от общей организации работы в конкретном подразделении.

В своей работе я буду рассматривать одну из программных средств защиты информации – антивирусные программы. Так, целью моей работы является проведение анализа антивирусных средств защиты информации. Достижение поставленной цели опосредуется решением следующих задач:

1) Изучение понятия антивирусных средств защиты информации;

2) Рассмотрение классификации антивирусных средств защиты информации;

3) Ознакомление с основными функциями наиболее популярных антивирусов.

Антивирусная программа (антивирус) — программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще, и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом (например, с помощью вакцинации).

Антивирусное программное обеспечение состоит из подпрограмм, которые пытаются обнаружить, предотвратить размножение и удалить компьютерные вирусы и другое вредоносное программное обеспечение.

Наиболее эффективны в борьбе с компьютерными вирусами антивирусные программы. Однако сразу хотелось бы отметить, что не существует антивирусов, гарантирующих стопроцентную защиту от вирусов, и заявления о существовании таких систем можно расценить как либо недобросовестную рекламу, либо непрофессионализм. Таких систем не существует, поскольку на любой алгоритм антивируса всегда можно предложить контр-алгоритм вируса, невидимого для этого антивируса (обратное, к счастью, тоже верно: на любой алгоритм вируса всегда можно создать антивирус).

Самыми популярными и эффективными антивирусными программами являются антивирусные сканеры (другие названия: фаг, полифаг, программа-доктор). Следом за ними по эффективности и популярности следуют CRC-сканеры (также: ревизор, checksumer, integritychecker). Часто оба приведенных метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа блокировщики и иммунизаторы.

Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Для поиска известных вирусов используются так называемые “маски”. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Если вирус не содержит постоянной маски, или длина этой маски недостаточно велика, то используются другие методы. Примером такого метода является алгоритмический язык, описывающий все возможные варианты кода, которые могут встретиться при заражении подобного типа вирусом. Такой подход используется некоторыми антивирусами для детектирования полиморфик - вирусов. Сканеры также можно разделить на две категории — “универсальные” и “специализированные”. Универсальные сканеры рассчитаны на поиск и обезвреживание всех типов вирусов вне зависимости от операционной системы, на работу в которой рассчитан сканер. Специализированные сканеры предназначены для обезвреживания ограниченного числа вирусов или только одного их класса, например макро-вирусов. Специализированные сканеры, рассчитанные только на макро-вирусы, часто оказываются наиболее удобным и надежным решением для защиты систем документооборота в средах MSWord и MSExcel.

Сканеры также делятся на “резидентные” (мониторы, сторожа), производящие сканирование “на-лету”, и “нерезидентные”, обеспечивающие проверку системы только по запросу. Как правило, “резидентные” сканеры обеспечивают более надежную защиту системы, поскольку они немедленно реагируют на появление вируса, в то время как “нерезидентный” сканер способен опознать вирус только во время своего очередного запуска. С другой стороны резидентный сканер может несколько замедлить работу компьютера в том числе и из-за возможных ложных срабатываний.

К достоинствам сканеров всех типов относится их универсальность, к недостаткам — относительно небольшую скорость поиска вирусов. Наиболее распространены в России следующие программы: AVP - Касперского, Dr.Weber – Данилова, NortonAntivirus фирмы Semantic.

Принцип работы CRC-сканеров основан на подсчете CRC-сумм (контрольных сумм) для присутствующих на диске файлов/системных секторов. Эти CRC-суммы затем сохраняются в базе данных антивируса, как, впрочем, и некоторая другая информация: длины файлов, даты их последней модификации и т.д. При последующем запуске CRC-

сканеры сверяют данные, содержащиеся в базе данных, с реально подсчитанными значениями. Если информация о файле, записанная в базе данных, не совпадает с реальными значениями, то CRC-сканеры сигнализируют о том, что файл был изменен или заражен вирусом. CRC-сканеры, использующие анти-стелс алгоритмы, являются довольно сильным оружием против вирусов: практически 100% вирусов оказываются обнаруженными почти сразу после их появления на компьютере. Однако у этого типа антивирусов есть врожденный недостаток, который заметно снижает их эффективность. Этот недостаток состоит в том, что CRC-сканеры не способны поймать вирус в момент его появления в системе, а делают это лишь через некоторое время, уже после того, как вирус разошелся по компьютеру. CRC-сканеры не могут определить вирус в новых файлах (в электронной почте, на дискетах, в файлах, восстанавливаемых из backup или при распаковке файлов из архива), поскольку в их базах данных отсутствует информация об этих файлах. Более того, периодически появляются вирусы, которые используют эту “слабость” CRC-сканеров, заражают только вновь создаваемые файлы и остаются, таким образом, невидимыми для них. Наиболее используемые в России программы подобного рода- ADINF и AVPInspector.

Антивирусные блокировщики — это резидентные программы, перехватывающие “вирусо-опасные” ситуации и сообщающие об этом пользователю. К “вирусо-опасным” относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения. Иногда некоторые функции блокировщиков реализованы в резидентных сканерах.

К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения, что, кстати, бывает очень полезно в случаях, когда давно известный вирус постоянно “выползает неизвестно откуда”. К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний, что, видимо, и послужило причиной для практически полного отказа пользователей от подобного рода антивирусных программ (например, неизвестно ни об одном блокировщике для Windows95/NT — нет спроса, нет и предложения).

Необходимо также отметить такое направление антивирусных средств, как антивирусные блокировщики, выполненные в виде аппаратных компонентов компьютера (“железа”). Наиболее распространенной является встроенная в BIOS защита от записи в MBR винчестера. Однако, как и в случае с программными блокировщиками, такую защиту легко обойти прямой записью в порты контроллера диска, а запуск DOS-утилиты FDISK немедленно вызывает “ложное срабатывание” защиты.

Существует несколько более универсальных аппаратных блокировщиков, но к перечисленным выше недостаткам добавляются также проблемы совместимости со стандартными конфигурациями компьютеров и сложности при их установке и настройке. Все это делает аппаратные блокировщики крайне непопулярными на фоне остальных типов антивирусной защиты.

Иммунизаторы - это программы записывающие в другие программы коды, сообщающие о заражении. Они обычно записывают эти коды в конец файлов (по принципу файлового вируса) и при запуске файла каждый раз проверяют его на изменение. Недостаток у них всего один, но он летален: абсолютная неспособность сообщить о заражении стелс-вирусом. Поэтому такие иммунизаторы, как и блокировщики, практически не используются в настоящее время. Кроме того многие программы, разработанные в последнее время, сами проверяют себя на целостность и могут принять внедренные в них коды за вирусы и отказаться работать.

КИБЕРПРЕСТУПНИКОВ НЕ ИНТЕРЕСУЮТ КОМПЬЮТЕРЫ ЧАСТНЫХ ЛИЦ

Личели Илья Давидович, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Киберпреступников не интересуют компьютеры частных лиц

К счастью, этому высказыванию мало кто верит. В данном случае утверждение также ложно.

Разумеется, корпоративные сети интересуют киберпреступников, но их сложнее заразить. Сегодня частные компьютеры так же хорошо подходят в качестве составляющих ботсетей. К тому же очень часто на них хранится много интересных персональных данных, таких как данные доступа к онлайн-магазинам, социальным сетям и учетным записям электронной почты или данные о кредитных картах, из которых киберпреступники могут извлечь выгоду. Поэтому не стоит недооценивать значение частных компьютеров для злоумышленников.

Большинство вредоносных программ распространяется по электронной почте

Данный тезис устарел, но, несмотря на это, данной точки зрения придерживается 54% участников опроса. В конце прошлого тысячелетия рассылка вирусов Melissa и I love you по электронной почте стала наиболее популярным способом распространения вредоносных программ. Приблизительно шесть лет назад на смену отправке электронных сообщении с зараженными вложениями пришли сообщения со ссылками на файлы, размещенные на Web-сайтах. Данная тактика позволяла злоумышленникам обходить очень эффективные спам-фильтры и доставлять сообщения ничего не подозревающему пользователю. С другой стороны, многие пользователи стали очень осторожны с сообщениями от неизвестных отправителей и в лучшем случае сразу удаляют их, не открывая. В большинстве случаев ссылки в электронных сообщениях направляют на вредоносные Web-сайты. Таким образом, появляются дополнительные возможности для поиска жертв: например, социальные сети, оптимизация поисковых запросов, ошибочные домены и т.д. Вредоносные программы находятся на Web-сайтах, а Web-сайты являются вектором заражения номер один.

Заражение ПК не происходит при загрузке зараженного Web-сайта

То, что почти половина интернет-пользователей считают данное утверждение правильным, шокирует. Заражение компьютера вредоносными кодами посредством вирусов "попутной загрузки" возможно уже на протяжении многих лет. Гипотеза о том, что одной лишь загрузки недостаточно для заражения, является опасным ложным заключением, данный вид атаки практикуется изо дня в день.

Существует два варианта заражения при "попутной загрузке".Во-первых, Web-сайты, созданные специально с целью заражения ПК.

Второй вариант более утонченный: вредоносный код внедряется на один из заслуживающих доверия популярных в настоящее время интернет-сайтов. Так, скажем, открывается незаметное для интернет-пользователя окно, например, размером 0x0 пикселей. Через это окно начинается загрузка, посредством которой происходит автоматическое и скрытое заражение ПК вредоносной программой. Преимуществом данного способа для киберпреступников является то, что им не приходится рекламировать Web-сайт. Для дальнейшей манипуляции данным Web-сайтом злоумышленникам необходимо в него внедриться. Если Web-сайт хорошо защищен, то осуществить такое внедрение очень сложно.

Большинство вирусов и вредоносных программ распространяются посредством зараженных файлов на файлообменниках

Бесспорно, определенное количество вредоносных программ распространяется через такие системы обмена файлами, как торренты и одноранговые сети. Неудивительно, что 48%

участников опроса считают, что данный способ является основным в распространении вредоносного ПО. Наверняка тот или другой пользователь уже хотя бы раз заражал свои компьютер вирусом после посещения подобных сайтов. Однако данный тезис также ложен и является мифом, поскольку большинство вредоносных программ распространяется через вредоносные Web-сайты.

Мой брандмауэр защищает меня от заражения при "попутной загрузке"

Данному утверждению верит 26% опрашиваемых. Этот тезис ложен. Брандмауэры – это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной Web-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных задании вредоносной программой и, например, отправку данных злоумышленникам, если речь идет о шпионских программах.

Если не открывать зараженные файлы, то ПК нельзя заразить

Это высказывание основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно лишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открытия зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

Большинство вредоносных программ распространяется через USB-накопители

В последние годы популярность флешек и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. Поэтому настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя.

) Я не посещаю странные Web-сайты, поэтому мне не угрожает заражение при "попутной загрузке"

Данное утверждение можно опровергнуть так же, как и шестой тезис. Тематика Web-сайта не играет для киберпреступников никакой роли. Они заинтересованы в том, чтобы с минимальными затратами заразить вредоносными кодами максимальное количество посетителей. Это удается злоумышленникам, помимо всего прочего, с помощью манипуляции с баннерами и постоянных атак крупных доменов. В случае успеха и получения доступа они внедряют вредоносный код с помощью так называемых эксплойт-инструментов, и специальные знания для этого не требуются. Web-саиты, которые на протяжении многих лет считались достойными доверия, могут быть взломанными и в результате таить в себе опасность заражения.

Обеспечение информационной безопасности в облачной инфраструктуре

При защите данных в публичном облаке, я выделяю два направления, так называемую безопасность облака, и безопасность в облаке. Безопасность в облаке обеспечивает провайдер, и мы на нее влиять никак не можем, поэтому здесь важно грамотно подойти к выбору поставщика облачных услуг и установлению с ним отношений. Для безопасности облака, в той части, где мы можем обеспечивать дополнительную безопасность, с помощью специальных программных средств и политик, сформулированы также свои рекомендации. Рассмотрены подходы к выбору облачного провайдера. Разработан ряд критериев по ИБ, которым должны соответствовать облачные провайдеры и на которые можно опираться при выборе поставщика облачных услуг.

Особое внимание уделено установлению партнерских отношений с провайдером, т.к. доверие к провайдеру и партнерские отношения исключительно важны, в том числе и для обеспечения ИБ данных. Доверие провайдеру очень важный пункт, но лучше чтобы дружба была подкреплена грамотно заключенным договором о предоставлении услуг и соглашением об уровне обслуживания (SLA). Данные документы могут иметь решающее значение при возникновении спорных ситуаций, в том числе связанных с ответственностью в вопросах ИБ.

Целостность информации

Реализация угроз информационной безопасности заключается в нарушении конфиденциальности, целостности и доступности информации. Злоумышленник может ознакомиться с конфиденциальной информацией, модифицировать ее, или даже уничтожить, а также ограничить или блокировать доступ легального пользователя к информации. При этом злоумышленником может быть как сотрудник организации, так и постороннее лицо. Но, кроме этого, ценность информации может уменьшиться ввиду случайных, неумышленных ошибок персонала, а также сюрпризов, иногда преподносимых самой природой.

РОЛЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лузганов Денис Владимирович, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В последние два десятилетия массовое производство персональных компьютеров и стремительный рост Интернета существенно ускорили становление информационного общества в развитых странах мира.

В информационном обществе главным ресурсом является информация, именно на основе владения информацией о самых различных процессах и явлениях можно эффективно и оптимально строить любую деятельность. Большая часть населения в информационном обществе занята в сфере обработки информации или использует информационные и коммуникационные технологии в своей повседневной производственной деятельности.

Для жизни и деятельности в информационном обществе необходимо обладать информационной культурой, т. е. знаниями и умениями в области информационных технологий, а также быть знакомым с юридическими и этическими нормами в этой сфере.

Информационный подход к исследованию мира реализуется в рамках информатики, комплексной науки об информации и информационных процессах, аппаратных и программных средствах информатизации, информационных и коммуникационных технологиях, а также социальных аспектах процесса информатизации.

Система (ОС), которая использует аппаратное и программное обеспечение, позволяющее компьютеру компенсировать нехватку физической памяти путем временной передачи данных из памяти произвольного доступа (ОЗУ) в дисковое хранилище. Виртуальное адресное пространство увеличивается за счет использования активной памяти в оперативной памяти и неактивной памяти на жестких дисках (HDD) для формирования смежных адресов, содержащих как приложение, так и его данные.

Виртуальная память разрабатывалась в то время, когда физическая память установленная оперативная память была дорогостоящей. Компьютеры имеют ограниченный объем оперативной памяти, поэтому память может заканчиваться, особенно когда одновременно выполняется несколько программ. Система, использующая виртуальную память, использует участок жёсткого диска для эмуляции оперативной памяти. С виртуальной памятью система может загружать большие программы или несколько программ, выполняющихся одновременно, позволяя каждой из них работать так, как будто она имеет бесконечную память и без необходимости приобретать больше оперативной памяти.

При копировании виртуальной памяти в физическую память операционная система разделяет память на файлы-страницы или файлы подкачки с фиксированным количеством адресов. Каждая страница хранится на диске, а когда она нужна, операционная система копирует ее с диска в основную память и преобразует виртуальные адреса в реальные адреса.

Адрес – это уникальный идентификатор местоположения какого-либо процесса внутри оперативной памяти. В ЭВМ адреса делятся на два типа: логический и физический. В начале исполнения программы для адресации данных в физическом адресном пространстве генерируют логические адреса. Далее сгенерированные логические адреса подаются на блок управления памятью (MMU, Memory Management Unit), находящийся в процессоре, который автоматически преобразовывает их в физические адреса. После этого можно говорить, что исполняемая программа полноценно находится в основной памяти. Таким образом, можно сказать, что логическим называется адрес, который «знает» программа.

Виртуальная память – это концепция, которая позволяет уйти от использования физических адресов, используя вместо них виртуальные.

Размер виртуального хранилища ограничен схемой адресации компьютерной системы, а объем вторичной памяти доступен не фактическим количеством основных хранилищ.

Это метод, который реализуется с использованием как аппаратного, так и программного обеспечения. Он отображает адреса памяти, используемые программой, называемые виртуальными адресами, в физические адреса в памяти компьютера.

Все ссылки на память в процессе являются логическими адресами, которые динамически преобразуются в физические адреса во время выполнения. Это означает, что процесс может быть выгружен из основной памяти и выгружен таким образом, что он занимает разные места в основной памяти в разное время в ходе выполнения.

Операционная система компьютера, используя комбинацию аппаратного и программного обеспечения, отображает адреса памяти, используемые программой, называемые виртуальными адресами, в физические адреса в памяти компьютера. Основное хранилище, видимое процессом или задачей, выглядит как непрерывное адресное пространство или совокупность непрерывных сегментов. Операционная система управляет виртуальными адресными пространствами и назначением реальной памяти виртуальной памяти. Аппаратное обеспечение преобразования адресов в ЦП, часто называемое блоком управления памятью (MMU), автоматически переводит виртуальные адреса в физические адреса. Программное обеспечение в операционной системе может расширять эти возможности для обеспечения виртуального адресного пространства, которое может превышать емкость реальной памяти и, таким образом, ссылаться на большее количество памяти, чем физически присутствует в компьютере.

Выглядит этот процесс следующим образом:

1. Сначала процессор подаёт на вход виртуальный адрес.
2. Если блок управления памятью выключен либо если виртуальный адрес попал в не транслируемую область, то физический адрес просто приравнивается к виртуальному.
3. Если блок управления памятью включен и виртуальный адрес попал в транслируемую область, то производится трансляция адреса, то есть замена номера виртуальной страницы на номер соответствующей ей физической страницы (смещение внутри страницы одинаковое).

Основные преимущества виртуальной памяти включают освобождение приложений от необходимости управлять общим пространством памяти, повышенную безопасность из-за изоляции памяти и возможность концептуально использовать больше памяти, чем физически доступно, используя технику подкачки.

Виртуальная память облегчает программирование приложений, скрывая фрагментацию физической памяти; делегируя ядру бремя управления иерархией памяти (устраняя необходимость явной обработки программой оверлеев); и когда каждый процесс выполняется в своем собственном выделенном адресном пространстве, устраняя необходимость перемещать программный код или обращаться к памяти с относительной адресацией.

Виртуальная память является неотъемлемой частью современной компьютерной архитектуры. Реализации обычно требуют аппаратной поддержки, как правило, в форме блока управления памятью, встроенного в ЦП. Хотя эмуляторы и виртуальные машины не являются необходимыми, они могут использовать аппаратную поддержку для повышения производительности своих реализаций виртуальной памяти.

Большинство современных операционных систем, которые поддерживают виртуальную память, запускают каждый процесс в своем собственном выделенном адресном пространстве. Таким образом, каждая программа имеет единственный доступ к виртуальной памяти. Однако некоторые старые операционные системы (такие как OS / VS1 и OS / VS2 SVS) и даже современные (такие как IBM i) являются операционными системами с единым адресным пространством, которые запускают все процессы в едином адресном пространстве, состоящем из виртуализированной памяти.

Встроенные системы и другие специализированные компьютерные системы, которые требуют очень быстрого и очень согласованного времени отклика, могут отказаться от использования виртуальной памяти из-за снижения детерминизма; Системы виртуальной памяти запускают непредсказуемые ловушки, которые могут вызвать нежелательные и непредсказуемые задержки в ответ на ввод, особенно если ловушка требует, чтобы данные считывались в основную память из вторичной памяти. Аппаратное обеспечение для преобразования виртуальных адресов в физические адреса обычно требует значительной площади чипа для реализации, и не все чипы, используемые во встроенных системах, включают это оборудование, что является еще одной причиной, по которой некоторые из этих систем не используют виртуальную память.

Сегментация – это ещё одна схема распределения несоприкасающейся памяти, например, пейджинг. Как и пейджинг, в сегментации процесс не делится произвольно на страницы монтируемого (фиксированного) размера. В сегментации вторичная и основная память не разделены на разделы одинакового размера. Разделы вторичной области памяти называются сегментами. Детали, касающиеся каждого сегмента, хранятся в таблице, известной как таблица сегментации. Таблица сегментов содержит две основные данные, касающиеся сегмента, одна - Base, которая является нижним адресом сегмента, а другая - Limit, которая является длиной сегмента.

При сегментации CPU генерирует логический адрес, который содержит номер сегмента и смещение сегмента. Если смещение сегмента меньше предела, то адрес называется допустимым адресом, в противном случае происходит просчет, так как адрес недействителен.

Некоторые системы, такие как Burroughs B5500, используют сегментацию вместо разбиения на страницы, разделяя виртуальные адресные пространства на сегменты переменной длины. Виртуальный адрес здесь состоит из номера сегмента и смещения внутри сегмента. Intel 80286 поддерживает аналогичную схему сегментации в качестве опции, но она используется редко. Сегментация и разбиение на страницы могут использоваться вместе, разделив каждый сегмент на страницы; В системах с такой структурой памяти, таких как Multics и IBM System / 38, обычно преобладает разбиение на страницы, сегментация обеспечивает защиту памяти.

В процессорах Intel 80386 и более поздних версиях IA-32 сегменты располагаются в 32-разрядном линейном страничном адресном пространстве. Сегменты могут быть перемещены в и из этого пространства; страницы могут «вставлять» в и из основной памяти, обеспечивая два уровня виртуальной памяти; немногие, если какие-либо операционные системы делают это, вместо этого используют только пейджинг. В ранних решениях по виртуализации x86 без аппаратной поддержки пейджинг и сегментация сочетались, потому что пейджинг x86 предлагает только два домена защиты, тогда как стеку VMM / гостевой ОС / гостевого приложения требуется три. Разница между системами подкачки и сегментации заключается не только в разделении памяти; сегментация видна пользовательским процессам как часть семантики модели памяти. Следовательно, вместо памяти, которая выглядит как одно большое пространство, она структурирована в несколько пространств.

Эта разница имеет важные последствия; сегмент - это не страница с переменной длиной или простой способ удлинить адресное пространство. Сегментация, которая может обеспечить одноуровневую модель памяти, в которой нет различия между памятью процесса и файловой системой, состоит только из списка сегментов (файлов), сопоставленных с потенциальным адресным пространством процесса.

Это не то же самое, что механизмы, предоставляемые вызовами, такими как mmap и WinView MapViewOfFile, потому что межфайловые указатели не работают при отображении файлов в полупроизвольные места. В Multics файл (или сегмент из многосегментного файла) отображается на сегмент в адресном пространстве, поэтому файлы всегда отображаются на границе сегмента. Раздел связывания файла может содержать указатели, для которых попытка загрузить указатель в регистр или сделать косвенную ссылку через него вызывает

ловушку. Неразрешенный указатель содержит указание имени сегмента, на который ссылается указатель, и смещение в пределах сегмента; обработчик для прерывания отображает сегмент в адресное пространство, помещает номер сегмента в указатель, изменяет поле тега в указателе, чтобы он больше не вызывал прерывание, и возвращает код, в котором произошла прерывание, повторно выполняя инструкция, которая вызвала ловушку. Это полностью устраняет необходимость в компоновщике и работает, когда разные процессы отображают один и тот же файл в разные места в своих частных адресных пространствах.

ИНСТРУМЕНТЫ ПОИСКА ОСТАТОЧНОЙ ИНФОРМАЦИИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Логунов Михаил Андреевич, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Остаточная информация — это данные или информация на запоминающем устройстве, которые осталась от формально удаленных операционной системой данных.

Остаточная информация включает в себя:

1. данные, найденные в нераспределенных блоках на носителе данных.
2. данные, найденные в свободном пространстве файлов и файловых систем.
3. данные в файлах, которые были технически удалены, так что они недоступны для приложения, использованного для создания файла.

Восстановление данных представляет собой процесс извлечения недоступных, потерянных, поврежденных, или отформатированных данных из вторичной памяти, сменных носителей или файлов , когда данные, сохраненные в них не могут быть доступны в обычном режиме. Данные чаще всего извлекаются с носителей, таких как внутренние или внешние жесткие диски, USB-накопители и другие электронные устройства. Восстановление может потребоваться из-за физического повреждения устройства хранения или логического повреждения файловой системы.

Есть два способа с помощью которых можно восстановить не перезаписанную информацию:

1. Программный
2. Программно-аппаратный

Программный способ – восстановление информации с использованием программного обеспечения без вмешательства в устройство накопителя. Этот способ может помочь в случаях:

1. Удаления информации
2. Форматировании диска

Программно-аппаратный – этот способ требуется при физическом повреждении накопителя.

Физический урон. Большое количество сбоев может привести к физическому повреждению носителей, что может быть вызвано человеческими ошибками. Жесткие диски могут пострадать от множества механических неисправностей, таких как поломка головки чтения/записи, неисправность печатной платы.

Большинство физических повреждений не могут быть устранены пользователями. Например, открытие жесткого диска в нормальных условиях может позволить пыли осесть на диск и оказаться зажатой между диском и головкой чтения/записи. Во время нормальной работы головки чтения/записи плавают на 3–6 нанометров над поверхностью пластины, а средние частицы пыли, обнаруженные в нормальной среде, обычно имеют диаметр около 30 000 нанометров. Когда эти частицы пыли попадают между головками чтения / записи и пластиной, они могут привести к новым поломкам головок, которые еще больше повреждают пластину и тем самым ставят под угрозу процесс восстановления.

Логический урон. В некоторых случаях данные на жестком диске могут быть нечитаемыми из-за повреждения таблицы разделов, файловой системы или ошибок носителя. В большинстве этих случаев, по крайней мере, часть исходных данных может быть восстановлена путем восстановления поврежденной таблицы разделов или файловой системы с использованием специализированного программного обеспечения для восстановления данных, такого как Testdisk.

Программы для поиска остаточной информации:

Recuva

Recuva - это условно-бесплатная утилита, которая способна восстанавливать потерянные (в результате программного сбоя или удаления) данных. Утилита была создана британской частной фирмой Piriform Limited и написана на C++.

Ее возможности:

1. Восстановление:
1. данных с поврежденных и отформатированных носителей информации.
2. удалённых сообщений из почтового ящика (поддерживает Microsoft Outlook Express, Mozilla Thunderbird и Windows Live Mail).
3. структуры папок.
4. несохранённых документов Microsoft Word.
2. Глубокое сканирование системы.
3. Расширенный и функциональный поиск файлов в системе, который способен:
1. показывать файлы из скрытых/системных папок.
2. показывать файлы с нулевым размером.
3. искать не удалённые файлы с повреждённых носителей.

Принцип работы

Данная программа после запуска и выбора параметров анализа предпринимает сканирование жёсткого диска на предмет поиска данных об оставшихся в системе файлах, не видимых для системы. Дело в том, что удаляя файл, система убирает от глаз пользователя его название и файл становится “невидимым”, хотя ещё какое-то время занимает некоторый объём памяти. Файл невозможно будет восстановить никакими средствами в том случае, если на место этого “невидимки” операционная система запишет новый, уже видимый для пользователя файл. То есть, Recuva обращается к памяти операционной системы и ищет невидимые файлы.

Disk Drill

Disk Drill - это утилита восстановления данных для Windows и macOS, разработанная Cleverfiles. Disk Drill был представлен в 2010 году и был в основном предназначен для восстановления удаленных или потерянных файлов с жестких дисков, USB-накопителей и SSD- дисков с помощью технологии Recovery Vault.

Она способна восстанавливать стёртые файлы за счёт функции Recovery Protection, а также находить файлы-дубликаты и очищать диск. Однако бесплатная версия не позволяет восстанавливать файлы, потерянные до установки Disk Drill.

Hetman Partition Recovery

Hetman Partition Recovery - условно-бесплатная программа для восстановления удаленных данных с разделов жесткого диска и других носителей. Утилита поддерживает как работающие диски, так и поврежденные логические разделы и восстанавливает данные как с переформатированных дисков, так и с дисков, для которых файловая система была изменена с FAT на NTFS или наоборот. Помимо работы с существующими разделами, инструмент также может находить удаленные логические диски, отображать их пользователю для дальнейшего поиска и восстановления удаленных файлов, а также исправлять ошибки в дизайне логических разделов.

Особенности

Утилита поддерживает файловые системы FAT12 / 16/32, NTFS и NTFS5 и обеспечивает восстановление основных форматов файлов, таких как документы, таблицы и презентации Microsoft Office и документы, электронные таблицы и презентации. Утилита так же может восстанавливать цифровые изображения, аудио- и видеофайл.

РОЛЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Лузганов Денис Владимирович, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В последние два десятилетия массовое производство персональных компьютеров и стремительный рост Интернета существенно ускорили становление информационного общества в развитых странах мира.

В информационном обществе главным ресурсом является информация, именно на основе владения информацией о самых различных процессах и явлениях можно эффективно и оптимально строить любую деятельность. Большая часть населения в информационном обществе занята в сфере обработки информации или использует информационные и коммуникационные технологии в своей повседневной производственной деятельности.

Для жизни и деятельности в информационном обществе необходимо обладать информационной культурой, т. е. знаниями и умениями в области информационных технологий, а также быть знакомым с юридическими и этическими нормами в этой сфере.

Информационный подход к исследованию мира реализуется в рамках информатики, комплексной науки об информации и информационных процессах, аппаратных и программных средствах информатизации, информационных и коммуникационных технологиях, а также социальных аспектах процесса информатизации.

Система (ОС), которая использует аппаратное и программное обеспечение, позволяющее компьютеру компенсировать нехватку физической памяти путем временной передачи данных из памяти произвольного доступа (ОЗУ) в дисковое хранилище. Виртуальное адресное пространство увеличивается за счет использования активной памяти в оперативной памяти и неактивной памяти на жестких дисках (HDD) для формирования смежных адресов, содержащих как приложение, так и его данные.

Виртуальная память разрабатывалась в то время, когда физическая память установленная оперативная память была дорогостоящей. Компьютеры имеют ограниченный объем оперативной памяти, поэтому память может заканчиваться, особенно когда одновременно выполняется несколько программ. Система, использующая виртуальную память, использует участок жёсткого диска для эмуляции оперативной памяти. С виртуальной памятью система может загружать большие программы или несколько программ, выполняющихся одновременно, позволяя каждой из них работать так, как будто она имеет бесконечную память и без необходимости приобретать больше оперативной памяти.

При копировании виртуальной памяти в физическую память операционная система разделяет память на файлы-страницы или файлы подкачки с фиксированным количеством адресов. Каждая страница хранится на диске, а когда она нужна, операционная система копирует ее с диска в основную память и преобразует виртуальные адреса в реальные адреса.

Адрес – это уникальный идентификатор местоположения какого-либо процесса внутри оперативной памяти. В ЭВМ адреса делятся на два типа: логический и физический. В начале исполнения программы для адресации данных в физическом адресном пространстве генерируют логические адреса. Далее сгенерированные логические адреса подаются на блок управления памятью (MMU, Memory Management Unit), находящийся в процессоре, который автоматически преобразовывает их в физические адреса. После этого можно говорить, что исполняемая программа полноценно находится в основной памяти. Таким образом, можно сказать, что логическим называется адрес, который «знает» программа.

Виртуальная память – это концепция, которая позволяет уйти от использования физических адресов, используя вместо них виртуальные.

Размер виртуального хранилища ограничен схемой адресации компьютерной системы, а объем вторичной памяти доступен не фактическим количеством основных хранилищ.

Это метод, который реализуется с использованием как аппаратного, так и программного обеспечения. Он отображает адреса памяти, используемые программой, называемые виртуальными адресами, в физические адреса в памяти компьютера.

Все ссылки на память в процессе являются логическими адресами, которые динамически преобразуются в физические адреса во время выполнения. Это означает, что процесс может быть выгружен из основной памяти и выгружен таким образом, что он занимает разные места в основной памяти в разное время в ходе выполнения.

Операционная система компьютера, используя комбинацию аппаратного и программного обеспечения, отображает адреса памяти, используемые программой, называемые виртуальными адресами, в физические адреса в памяти компьютера. Основное хранилище, видимое процессом или задачей, выглядит как непрерывное адресное пространство или совокупность непрерывных сегментов. Операционная система управляет виртуальными адресными пространствами и назначением реальной памяти виртуальной памяти. Аппаратное обеспечение преобразования адресов в ЦП, часто называемое блоком управления памятью (MMU), автоматически переводит виртуальные адреса в физические адреса. Программное обеспечение в операционной системе может расширять эти возможности для обеспечения виртуального адресного пространства, которое может превышать емкость реальной памяти и, таким образом, ссылаться на большее количество памяти, чем физически присутствует в компьютере.

Выглядит этот процесс следующим образом:

4. Сначала процессор подаёт на вход виртуальный адрес.
5. Если блок управления памятью выключен либо если виртуальный адрес попал в не транслируемую область, то физический адрес просто приравнивается к виртуальному.
6. Если блок управления памятью включен и виртуальный адрес попал в транслируемую область, то производится трансляция адреса, то есть замена номера виртуальной страницы на номер соответствующей ей физической страницы (смещение внутри страницы одинаковое).

Основные преимущества виртуальной памяти включают освобождение приложений от необходимости управлять общим пространством памяти, повышенную безопасность из-за изоляции памяти и возможность концептуально использовать больше памяти, чем физически доступно, используя технику подкачки.

Виртуальная память облегчает программирование приложений, скрывая фрагментацию физической памяти; делегируя ядру бремя управления иерархией памяти (устраняя необходимость явной обработки программой оверлеев); и когда каждый процесс выполняется в своем собственном выделенном адресном пространстве, устраняя необходимость перемещать программный код или обращаться к памяти с относительной адресацией.

Виртуальная память является неотъемлемой частью современной компьютерной архитектуры. Реализации обычно требуют аппаратной поддержки, как правило, в форме блока управления памятью, встроенного в ЦП. Хотя эмуляторы и виртуальные машины не являются необходимыми, они могут использовать аппаратную поддержку для повышения производительности своих реализаций виртуальной памяти.

Большинство современных операционных систем, которые поддерживают виртуальную память, запускают каждый процесс в своем собственном выделенном адресном пространстве. Таким образом, каждая программа имеет единственный доступ к виртуальной памяти. Однако некоторые старые операционные системы (такие как OS / VS1 и OS / VS2 SVS) и даже современные (такие как IBM i) являются операционными системами с единым адресным пространством, которые запускают все процессы в едином адресном пространстве, состоящем из виртуализированной памяти.

Встроенные системы и другие специализированные компьютерные системы, которые требуют очень быстрого и очень согласованного времени отклика, могут отказаться от использования виртуальной памяти из-за снижения детерминизма; Системы виртуальной памяти запускают непредсказуемые ловушки, которые могут вызвать нежелательные и непредсказуемые задержки в ответ на ввод, особенно если ловушка требует, чтобы данные считывались в основную память из вторичной памяти. Аппаратное обеспечение для преобразования виртуальных адресов в физические адреса обычно требует значительной площади чипа для реализации, и не все чипы, используемые во встроенных системах, включают это оборудование, что является еще одной причиной, по которой некоторые из этих систем не используют виртуальную память.

Сегментация – это ещё одна схема распределения несоприкасающейся памяти, например, пейджинг. Как и пейджинг, в сегментации процесс не делится произвольно на страницы монтируемого (фиксированного) размера. В сегментации вторичная и основная память не разделены на разделы одинакового размера. Разделы вторичной области памяти называются сегментами. Детали, касающиеся каждого сегмента, хранятся в таблице, известной как таблица сегментации. Таблица сегментов содержит две основные данные, касающиеся сегмента, одна - Base, которая является нижним адресом сегмента, а другая - Limit, которая является длиной сегмента.

При сегментации CPU генерирует логический адрес, который содержит номер сегмента и смещение сегмента. Если смещение сегмента меньше предела, то адрес называется допустимым адресом, в противном случае происходит просчет, так как адрес недействителен.

Некоторые системы, такие как Burroughs B5500, используют сегментацию вместо разбиения на страницы, разделяя виртуальные адресные пространства на сегменты переменной длины. Виртуальный адрес здесь состоит из номера сегмента и смещения внутри сегмента. Intel 80286 поддерживает аналогичную схему сегментации в качестве опции, но она используется редко. Сегментация и разбиение на страницы могут использоваться вместе, разделив каждый сегмент на страницы; В системах с такой структурой памяти, таких как Multics и IBM System / 38, обычно преобладает разбиение на страницы, сегментация обеспечивает защиту памяти.

В процессорах Intel 80386 и более поздних версиях IA-32 сегменты располагаются в 32-разрядном линейном страничном адресном пространстве. Сегменты могут быть перемещены в и из этого пространства; страницы могут «вставлять» в и из основной памяти, обеспечивая два уровня виртуальной памяти; немногие, если какие-либо операционные системы делают это, вместо этого используют только пейджинг. В ранних решениях по виртуализации x86 без аппаратной поддержки пейджинг и сегментация сочетались, потому что пейджинг x86 предлагает только два домена защиты, тогда как стеку VMM / гостевой ОС / гостевого приложения требуется три. Разница между системами подкачки и сегментации заключается не только в разделении памяти; сегментация видна пользовательским процессам как часть семантики модели памяти. Следовательно, вместо памяти, которая выглядит как одно большое пространство, она структурирована в несколько пространств.

Эта разница имеет важные последствия; сегмент - это не страница с переменной длиной или простой способ удлинить адресное пространство. Сегментация, которая может обеспечить одноуровневую модель памяти, в которой нет различия между памятью процесса и файловой системой, состоит только из списка сегментов (файлов), сопоставленных с потенциальным адресным пространством процесса.

Это не то же самое, что механизмы, предоставляемые вызовами, такими как mmap и WinView MapViewOfFile, потому что межфайловые указатели не работают при отображении файлов в полупроизвольные места. В Multics файл (или сегмент из многосегментного файла) отображается на сегмент в адресном пространстве, поэтому файлы всегда отображаются на границе сегмента. Раздел связывания файла может содержать указатели, для которых попытка загрузить указатель в регистр или сделать косвенную ссылку через него вызывает

ловушку. Неразрешенный указатель содержит указание имени сегмента, на который ссылается указатель, и смещение в пределах сегмента; обработчик для прерывания отображает сегмент в адресное пространство, помещает номер сегмента в указатель, изменяет поле тега в указателе, чтобы он больше не вызывал прерывание, и возвращает код, в котором произошла прерывание, повторно выполняя инструкция, которая вызвала ловушку. Это полностью устраняет необходимость в компоновщике и работает, когда разные процессы отображают один и тот же файл в разные места в своих частных адресных пространствах.

ПОВАРЕННАЯ КНИГА МАТЕМАТИКИ

Майкова Ксения Федоровна, Щуров Андрей Владимирович, студенты 1-го курса
Научный руководитель Боровская Ираида Владимировна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Все мы прекрасно знаем, что математика присутствует во многих сферах в нашей жизни. Но как насчет кулинарии? Есть ли там математика? Представляем вашему вниманию, кулинария с точки зрения математики!

Мы знаем, что для приготовления любого блюда должен соблюдаться рецепт. В рецепте берется точное соотношение продуктов, которое необходимо соблюдать в процессе приготовления. Математические величины масса и объём используют при взвешивании продуктов. Еще нужно помнить о единицах времени. Берем рецепт какого-либо блюда, например, борща с говядиной, нужную нам формулу и проводим сложные математические вычисления. В нашем случае мы не будем учитывать графу уксус и перец, потому что они по вкусу.

Но с другой стороны, математика — это точная наука, а в кулинарии нет никакой точности, каждый чувствует все по-своему и продукты не могут быть полностью одинаковыми. В этом и главная проблема.

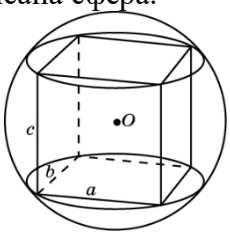
Но тут стоит вспомнить, что математика — это не только сложные алгебраические вычисления, но и так же геометрические. Геометрия уже больше подходит к кулинарии, не правда ли?

Геометрия очень сильно преобладает в кулинарии: в нарезке овощей для приготовления супов, салатов, вторых блюд, десертов.

Так же не с точки зрения эстетичности блюда, а по большой части правильного усвоения и приготовления пищи.

Но вопрос в том, какие формулы или законы надо применить, чтобы приготовить настоящий шедевр? На самом деле сейчас нам понадобятся лишь формулы для параллелепипеда. Возьмем для примера один из них.

В прямоугольный параллелепипед вписана сфера.



Вот его формула площади полной поверхности, объёма, радиуса вписанной сферы:

$$S = 6 \cdot a^2; \quad V = a^3; \quad r = \frac{a}{2}.$$

И так, мы имеем многогранник формулы к нему, можно найти его объём и радиус вписанной сферы.

А давайте приготовим идеальный геометрический десерт с помощью наших вычислений?

Хорошо, отойдем от темы кулинарии и ближе рассмотрим пропорции. Казалось бы, пропорции – одни из самых простых вещей в математике, да это так, но все намного глубже.

Приготовленные блюда нужно правильно делить на порции, в чём нам опять же помогает математика. Для того чтобы пользоваться кулинарными рецептами и производить перерасчет продуктов по ним, порой требуется знать, что такое отношение, пропорциональность.

«Вообще-то, незначительные детали обычно важнее всего» - сказал Шерлок Холмс[1]. Пропорции являются маленькой деталькой в большом механизме. Как мы уже знаем, пропорции есть везде и это значит, что пропорции являются неотъемлемой частью всего. Означает ли это, что благодаря пропорциям можно сделать много великих вещей? На самом деле пропорция – это больше инструмент для тех великих вещей. Это доказывает ее важность, и ее неотъемлемость.

Еще одно неожиданное применение пропорции мы нашли в музыке. Ученные проанализировали композиции великих музыкантов и установили, что в них присутствуют законы золотого сечения.

Сложно придумать сферу, где вообще не присутствует или хотя бы частично присутствует математика.

Даже наше с вами восприятие красоты основаны на математических пропорциях или по другому в золотом сечении.

Подытожив все выше сказанное можно сделать вывод о том, что математика, в каких-то ее проявлениях все-таки присутствует в кулинарии и абсолютно каждый может в этом убедиться. Математика – это многогранная наука, присутствие ее в многих сферах нашей жизни очевидно, только надо немного присмотреться.

Список использованных источников

1. Дорофеев Г. В., Седова Е. А. Процентные вычисления. Учебное пособие для старшеклассников. М.: Дрофа, 2003
2. Здобнов А.И. Сборник рецептов блюд и кулинарных изделий. – М.: Лада, 2010
3. Канторович Г.Г., Денищева Л.О., Краснянская К.А. ЕГЭ -2009 по математике // Математика в школе. 2009.
4. Лысенко Е.А., Тонких А.П. Занимательная математика. – М.: Просвещение, 2006
5. Перельман Я.И. Как сделать изучение геометрии интересным и жизненным? // Математика в школе. 2008г.
6. Сергеев И.С. «Примени математику»
7. https://citatnica.ru/citaty/tsitaty-iz-filma-sherlok-holms-200-tsitat
8. http://heerdjaws.blogspot.ru/2012/11/blog-post_4119.html
9. http://www.magic-cook.com/forum/viewtopic.php?p=1766
10. http://www.workchild.30nar-s2.edusite.ru/ovosch/narezannie_ovoshi.html
11. https://math.wikireading.ru/2268
12. http://www.hintfox.com/article/printsip-zolotogo-sechenija-i-ego-projavlenie-v-myzike-kompozitorov-klassikov.html

РЕЗЕРВНОЕ КОПИРОВАНИЕ И ВОССТАНОВЛЕНИЕ РЕЕСТРА ОС WINDOWS

Макушина Кристина Вячеславовна, студент 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Выполнение программ является главной задачей ЭВМ. Чтобы внести какие-либо изменения в операционную систему, надо внести изменения в реестр. В операционной системе при работе с программами часто вносятся изменения в записи реестра. Сами программы вносят изменения, а также и пользователи. Пользователи при редактировании реестра, когда удаляют программы или вносят изменения в настройках вручную, а сами программы при своей работе.

Актуальность темы в том, что часто компьютер тормозит или не хочет запускаться. Проблема часто указывает на реестр Windows, потому что это основной элемент операционной системы. От него зависит работа множество установленных программ. В связи с этим ошибки с реестром могут помешать работе всего компьютера.

Реестр впервые появился в выпущенной в 1933 году версии Windows NT 3.1. С появлением системы NTFS, проблемы которые решал реестр исчезли. Microsoft Windows – это единственная операционная система где остался реестр и используется на сегодняшний день во всех версиях.

Реестр – это большая база данных, в которой хранятся настройки и параметры аппаратного обеспечения в самой операционной систем и аппаратного обеспечения компьютера (например, драйвера, настройки драйверов, настройки каких-то программ и настройки самой операционной системы).

Реестр состоит из ключей с определенными настройками, эти ключи выглядят как папки и хранятся в визуальном редакторе реестра.

Windows управляет процессами, происходящими при работе приложений и устройств компьютера. Для повышения оперативности ОС использует базу данных, хранящую актуальную информацию о настройках и конфигурации программного обеспечения и внешних устройств. Любые действия, изменяющие внешний вид либо изменение каких-либо настроек, по сути, изменяются параметры в самом реестре. Инструменты с работой реестра – это и есть меню Windows. Самым основным инструментом реестра Windows является «Редактор реестра».

Реестр - это не статическая база данных, он постоянно работает и обновляется. При запуске любой программы происходит множество обращений к реестру, еще больше обращений происходит при запуске компьютера. Реестр имеет важное значение для более эффективной работы компьютера. Если реестр замусорен, то это является главной причиной изменений работы компьютера и снижение, замедление скорости Windows. На данный момент главный вопрос как ускорить в нём работу, усовершенствовать создание файлов реестра и внесение файлов реестра внутрь системы.

Самая важная рекомендация для пользования реестра – это если мы не знаем для чего, он нужен или если редактируем параметры, то мы должны знать для чего это нужно и без надобности не стоит редактировать. Обычно это приводит к сбою в системе и в каждой новой операционной системе появляются новые параметры, при этом остаются рабочие и предыдущие. Часть параметров становится не актуальной.

Описание логической структуры включает в себя анализ пяти основных разделов реестра в том виде, в каком они отображаются в основных редакторах реестра Windows. Структура включает в себя то, как и где файлы кустов реестра хранятся в физической памяти.

Когда происходит запуск операционной системы, также происходит множество обращений к реестру, а во время работы на компьютере в течение одного сеанса работы – до 10 тысяч. Очень часто происходит считывание в реестр информации. Например, если мы

скачиваем какую-либо программу, информация, которая нужна, нам для запуска программы записывается в реестр операционной системы.

Реестр Windows был создан для сгруппирования информации хранившихся в текстовых INI – файлах. В файловой системе Windows FAT16 поиск по директориям был медленным, поэтому в версии Windows 3.1 заменили INI – файлы на реестр. С массовым переходом Windows на файловую систему NTFS проблема с поиском по каталогам ушла и сегодняшний день Windows — единственная операционная система, которая имеет реестр.

Лучше заниматься редактированием с помощью специальных программ – они предотвращают большую часть изменений, влияющих на работу Windows.

Реестр имеет иерархическую структуру, которая состоит из разделов, подразделов и параметров. В редакторе реестра находятся пять основных ключевых разделов, они выглядят как папки и каталоги. Каждый раздел состоит из подразделов.

Первой операционной системой для компьютеров от Microsoft была MS- DOS. В ней было два основных файла: config.sys и autoexec.bat. Первый содержал инструкции по загрузке драйверов и программ. В autoexec.bat указывались команды, которые выполнялись при загрузке DOS.

Windows 3.1 вышла в 1993 году – графическая оболочка для операционной системы MS- DOC. В этой версии произошло много улучшений и появилась новая функция: реестр. Он имел только один куст HKEY_CLASSES_ROOT. Когда появился реестр, также появилась и программа для редактирования реестра: REGEDIT.EXE. Реестр в Windows 3.1 имел ограничения по размеру – 64 Кбайт. Если же реестр превышал размер, то файл реестра приходилось удалять.

В Windows NT 3.1 произошел отказ от устаревших файлов MS- DOC и от INI-файлов. Основным видом системы стал реестр. Он имел уже 4 раздела: HKEY_ LOCAL_MACHINE, HKEY_CURRENT_USER, HKEY_CLASSES_ROOT и HKEY_USERS.

Версии реестра для разных версий операционных систем Windows имеют отличия. Данные реестра хранятся в двоичных файлах.

Главное отличие версий Windows Vista/ Windows 7/ Windows Server 2008 от старых версий в том, что появляется новый раздел HKEY_LOCAL_MACHINE \BCD00000000. Раздел HKEY_CURRENT_CONFIG впервые появился в Windows NT 4.0. В Windows 10 существенных изменений в реестре не было. В современном реестре часть данных хранится в файлах, а другая часть порождается в процессе загрузки Windows. После редактирования реестра или внесения в него изменений, они сразу же записываются в файлы, где и хранятся.

В наше время пользователи очень любят скачивать много программ из Интернета, uTorrent, так же покупать гифки с различными программами и играми, сайты с которых все скачивают в нашей стране все равно остаются пиратскими. Устанавливая, какое-либо программное обеспечение или игры пользователь может занести в свой компьютер вирусы, либо полное падение системы, а также глюки, которые могут возникать абсолютно в любых программах. Например, пользователь скачивает какую-то игру или программу, она не запускается и еще после этого происходят неполадки в операционной системе. Пользователь обычно в этих случаях пытается удалить эту программу или игру, но при этом все неприятности, которые он занес не проходят и некуда не исчезают. Причина всего этого одна. Даже если мы удалим эту программу, то в этом случае в реестре операционной системы все равно остаются какие-либо ключи, коды или какие-нибудь остатки от той программы или игры, которую устанавливали. Реестр в любом случае уже будет заполнен какими-нибудь самыми непредвиденными ключами, которые могут запускать дополнительные процессы не нужные системе, из-за которых она может тормозить, перезагружаться или работать неправильно, либо сбивать другие программы. Причем во многих случаях даже программы чистки реестра от остатка других программ, которые уже удалены, в этом случае могут не помочь и соответственно все неприятности могут даже после удаления не сработавшей программы останутся. Единственный способ обезопасить от

таких проблем это создание резервной копии реестра, перед тем как установить на компьютер, какую либо или программу и это обезопасит компьютер.

Процесс создания резервной копии реестра Windows очень простой. Иметь резервную копию реестра необходимо, в случае если редактировать что-либо в реестре может привести к серьезным последствиям, которые нежелательны.

Когда мы делаем резервную копию реестра, можем выбрать тип файла, то есть формат:

- Файлы реестра (*.reg);
- Файлы кустов реестра(*.*);
- Текстовые файлы(*.txt), можно прочитать в блокноте;
- Файлы реестра Win9x/NT4(*.reg);
- Все файлы;

В любой момент мы можем восстановить резервную копию, но не всегда это может получиться. Восстановление реестра Windows делается с помощью функции «импорт» в редакторе реестра либо через Reg-файл в том месте, куда сохранилась резервная копия реестра Windows.

Существуют специальные программы, которые позволяют восстанавливать реестр, например Recovery Toolbox for Registry, Vit Registry Fix Free Edition 9.5.9, Auslogics Registry Cleaner.

Самая распространенная программа для восстановления реестра Windows - программа ERUNT. Это надежный и проверенный временем инструмент для сохранения и быстрого его восстановления реестра Windows. Многие пользователи предпочитают заменять им стандартную функцию восстановления системы, так как он практически не дает сбоев, не расходует системные ресурсы и не требует большого количества свободного места на жестком диске.

Есть еще одна бесплатная утилита для копирования и восстановления реестра Windows называется она TweakingRegistryBackup.

Однако, более разумным и эффективным способом, наверное, является включение создания точек восстановления Windows , которые будут содержать, в том числе, и работающий вариант реестра.

Сбои в работе ПК возможны и после установки программных решений, которые требуют совершения изменений в системной базе данных. Также бывают ситуации, когда юзер случайно удаляет целый подраздел реестра, что приводит к нестабильной работе ПК и чтобы устранить подобные проблемы, производится восстановление реестра.

Применяя данные методы, можно произвести процесс восстановления реестра в рабочее состояние. Также хочется отметить, что время от времени необходимо создавать точки восстановления и резервные копии реестра.

При работе с реестром нет никаких сложностей, даже для новеньких. Следует соблюдать осторожность и не совершать ошибок с внесением изменений в реестр, а также помнить, что любые не обдуманные действия могут иметь серьезные последствия. Лучше всего создавать резервную копию изменяемых параметров, при которой можно, если что восстановить реестр в операционной системе Windows.

Анализ работы реестра доказывает необходимость существования его в операционной системе.

Перед внесением каких-либо изменений, необходимо обязательно сделать резервную копию и обдуманно делать изменения в реестре Windows. Кроме этого, после внесения изменений в реестре, может пойти что-то не так и всегда можно восстановить копию реестра. Нельзя оставить без внимания тот факт, что существует множество программ для восстановления и копирования реестра Windows.

В заключении хочется подтвердить, реестр Windows – это огромное хранилище данных, позволяющее стабильно работать операционной системе Windows.

В настоящее время необходимость реестра в операционной системе Windows очень актуальна, работать с ним надо аккуратно и обдуманно.

Список использованных источников

1. Основы операционных систем/ К.А. Коньков, В.Е. Карпов – М.: НациональныйОткрытый Университет «ИНТУИТ», 2016
2. Справочник реестр Microsoft Windows/ Климов Александр, Чеботарёв Игорь, 2009
3. «Реестр Microsoft Windows XP. Руководство профессионала», Джерри Хонейкатт, изд. Эком, Москва, 2003
4. «Реестр Windows XP», Куприянова А.В., 2005
5. Резервное копирование и восстановление [электронный ресурс]
6. Олифер В.Г., Олифер Н.А. Сетевые операционные системы: Учебник для вузов. - СПб.:Питер, 2006.
7. Эндрю Таненбаум Современные операционные системы. 2-е изд.-СПб.: Питер. 2007.

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ РАСКРОЙКИ ЗАГОТОВКИ НА УЧАСТКЕ ПИЛ ХОЛОДНОЙ РЕЗКИ СПЦ-1 АО «ОЭМК ИМ. А.А.УГАРОВА»

Малышенко Сергей Андреевич, студент 4-го курса
Научный руководитель Азарова Виктория Сергеевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Режущие пилы для холодного металла предназначены для быстрой резки отрезков или кусков оцинкованного стального листа без нагрева лезвия или материала

Целью исследования является расширенный анализ АСУ раскройки заготовки на участке пил холодной резки СПЦ-1 АО «ОЭМК им. А.А.Угарова.

Задачи исследования:

- изучить характеристику технологического процесса участка пил холодной резки и его технологические параметры;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является раскройки заготовки на участке пил холодной резки СПЦ-1 АО «ОЭМК им. А.А.Угарова».

Продукция ОЭМК соответствует международной системе менеджмента качества ISO 9100. Данный участок позволяет произвести снятия пробы с готовой продукции, а также раскроя заготовок в соответствии с требованиями заказчика.

Оборудование, установленное на участке ПХР:

Bero 0 - датчик занятости (рольганг загружен)

Bero 1 - заготовка перед рольгангом 1 ролик 8

Bero 2 - рольганг 2 на конце загружен

BLS1 - световой барьер для опускания измерительного ролика

BLS2 - синхронизирующий световой барьер

GFS-A - частотный преобразователь для рольганга 1

GFS-B - частотный преобразователь для рольганга 2

Гр.1.1, Гр.1.2, Гр.2.2, Гр.2.1 - силовые коммутационные пускатели.

Схема расположения оборудования на участке ПХР представлена на рисунке 1.

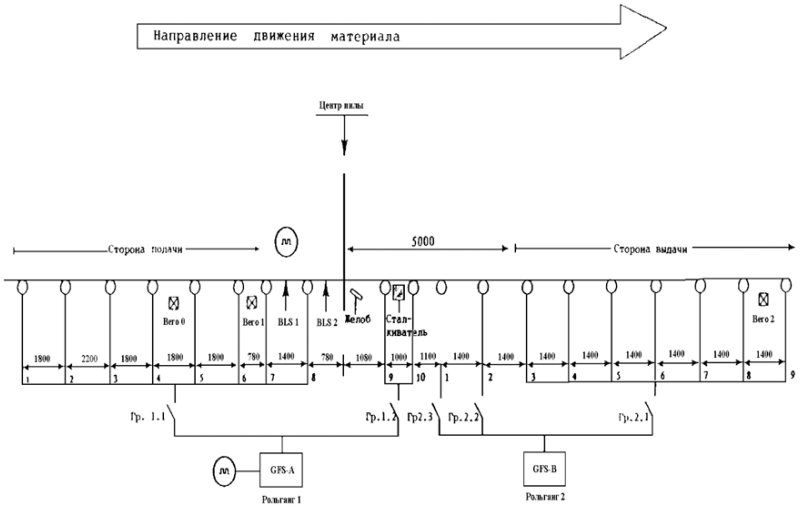


Рисунок 1 - Схема расположения оборудования на участке ПХР

Основные требования к обрабатываемому прокату

Раскрой заготовки производится в холодном состоянии.

Раскройке подлежит прокат круглого сечения диаметром 80 - 180 мм.

Длина проката - не более 12м.

Поверхностные дефекты должны быть удалены на зачистных станках или обточных установках участка отделки СПЦ-1.

Кривизна проката -не более 5мм/м. Кривизна проката обеспечивается технологией производства проката и не контролируется.

Функциональная схема раскроя заготовки представлена на рисунке 2.

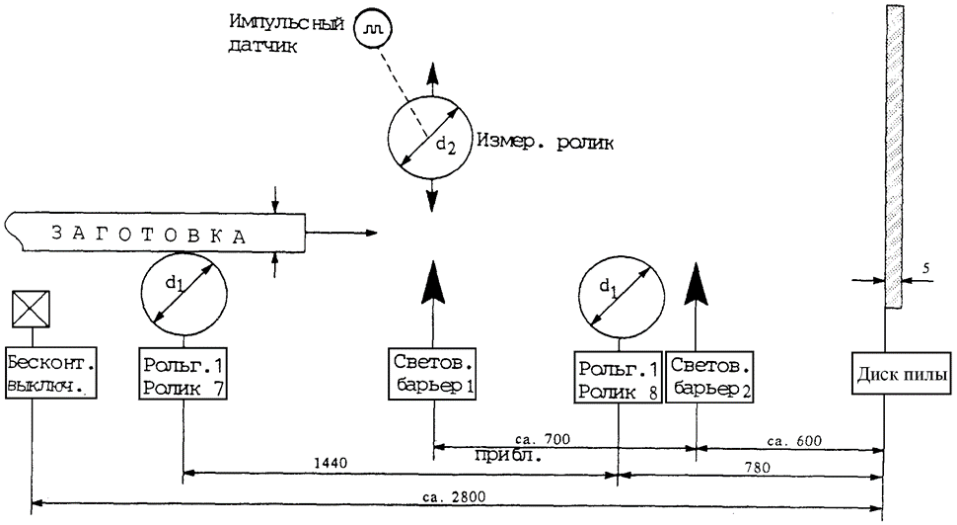


Рисунок 2 - Функциональная схема раскроя заготовки

Процесс раскройки выглядит следующим образом: заготовка поступает на рольганг с помощью подъемного шлеппера, при поступлении заготовки на рольганг включается автоматизированная система контроля и измерения длины. Необходимым условием перед началом позиционирования является:

- Сигнал с концевых о том, что суппорт пилы находится в начальной позиции.
- Сигнал с концевых о том, что вертикальные и горизонтальные зажимы отведены.
- Сигнал с концевых о том, что датчик находится в верхнем положении.
- Сигнал с концевых о том, что желоб и сталкиватель находится в нижнем положении.

Длина заготовки измеряется с помощью измерительного ролика, который опускается на заготовку при прохождения заготовки через первый световой барьер. В момент прохождения второго светового барьера начинается измерение длины заготовки, при чем расстояние между световым барьерам и диском пилы постоянно и в дальнейшем используется в расчете точки начала торможения. процесс торможения осуществляется преобразователем частоты при этом время замедления заготовки от 100% до 0 определяется параметрами преобразователя, данная величина постоянна. Длина торможения не зависит от массы заготовки, так как процесс торможения полностью контролируется преобразователем. После чего заготовка фиксируется зажимными колодками в горизонтальной и вертикальной плоскости, затем производится раскройка. По окончании процесса раскройки производят развод пропила, что позволяет свободно осуществить вывод диска пилы из зоны раскроя. После выхода пильного диска из зоны раскройки зажимные колодки разводятся, и заготовка транспортируется дальше.

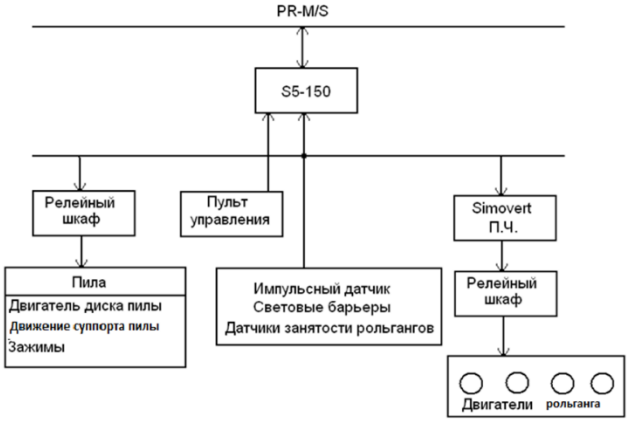
В состав оборудования ПХР входит:

- подводящий рольганг
- пила холодной резки:
- суппорт пилы с приводом и механизмом переключения передач;
- пильный диск;
- привод пильного диска;
- стружкосъемник;

- амортизатор;
- устройство для охлаждения диска;
- кожух диска
- механизм зажима заготовки (вертикальный и горизонтальный зажимы);
- транспортер стружки;
- устройство измерения длины;
- отводящий рольганг..

В настоящий момент процесс позиционирования заготовки на участке пил холодной резки контролирует SIMATIC S5-150, и процесс полностью автоматизирован. Измерение длины происходит посредством импульсного датчика, следующим образом: при поступлении заготовки на датчик занятости включается рольганг, первый световой барьер обеспечивает опускание измерительного ролика, а второй световой барьер синхронизацию счетчиков.

Имеющаяся автоматизированная система управления, рисунок 3, трехуровневая и состоит из нижнего уровня (датчиков и исполнительных механизмов), среднего (уровня контроллера), верхнего (система слежения) общающихся между собой с помощью промышленной сети Profibus и индустриальной сети Ethernet.



Такой способ измерения имеет ряд следующих недостатков:

Неравномерный износ по ширине измерительного ролика на разных диаметрах заготовки, приводит к увеличению погрешности измерений. Кроме того, существенным недостатком является то, что при опускании измерительного ролика на заготовку происходит удар об нее, что в дальнейшем сказывается на систему измерений. Следующим недостатком существующего метода замера длины заготовки является то, что измерительный ролик соединен с импульсным датчиком посредством карданного вала с двумя гибкими муфтами, что приводит к увеличению люфтов в соединении. А также сам датчик имеет низкую надежность, и происходят пропуски в импульсах. Данные недостатки приводят к тому, что при измерении контролируется оператором каждая заготовка по шаблону, что отражается на производительность участка.

Слежение за металлом осуществляется с помощью светового барьера типа PP2009/2e2 и датчиков занятости Bero. Управление двигателями рольганга осуществляется при помощи частотного преобразователя типа 6SC и силовых коммутационных пускателей. Данный частотный преобразователь устарел и кроме того дорогой в эксплуатации.

В ходе модернизации предлагается ряд технических решений, позволяющих исключить факторы негативно влияющие на эффективность работы установки. К ним относятся:

- замена существующих аппратаных средств измерения длины заготовки;
- замена существующей систем автоматизации, выполненной на базе контроллера Simatic S5 на систему на базе более совершенного Simatic S7;
- разработка и внедрение SCADA системы визуализации;

Данные изменение позволят:

- обеспечить порез с минимальной погрешностью;

- увеличит надежность системы;
- уменьшит вероятность ошибки оператора;
- внедрение визуализации позволит оператору видеть процесс в реальном времени.

В итоге модернизация системы позиционирования раскроя заготовки позволит значительно снизить затраты на ремонт и экономические потери, увеличить производительность участка.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств [Текст]: учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Суркова Л. Е. Моделирование систем автоматизации и управления технологическими процессами : практикум / Л. Е. Суркова, Н. В. Мокрова. - Саратов: Вузовское образование, 2019. - 46 c. - ISBN 978-5-4487-0496-3. - Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - URL: http://www.iprbookshop.ru/82692.html. - Режим доступа: для авторизир. пользователей

4. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. - 2-е изд. - Саратов : Ай Пи Эр Медиа, 2019. - 459 c. - ISBN 978-5-4486-0574-1. - Текст: электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. - URL: http://www.iprbookshop.ru/83341.html. - Режим доступа: для авторизир. пользователей

ТРАНКИНГОВЫЕ СИСТЕМЫ СВЯЗИ

Матюнькин Димитрий Александрович, курсант 3 курса
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Одной из основных тенденций развития систем связи является поиск наиболее эффективных путей использования частотного диапазона. Это положительно скажется как на удобстве пользования, так и на положении дел с возможностью выделения частот.

Слово «транк» происходит от английского trunk – пучок, символ, в телефонии этот термин означает «магистраль».

Транкинг – это совокупность каналов связи, автоматически распределяемых между пользователями. В обычной системе за группой пользователей «А» закреплен канал А, за группой «В» – канал В и т.д. Если пользователь из группы «А» обнаруживает, что канал А занят, то с этим ничего нельзя поделать, даже если канал В свободен. В результате этого пожарная машина или скорая помощь, оснащенная такой системой, приезжает на сорок минут позже, а милицейская не приезжает вообще, потому что ловить преступника уже поздно.

В транкинговых системах вместо одного канала, к которому обращается несколько пользователей, содержится группа каналов (символ), доступных всем пользователям данной системы. Когда кто-либо из них захочет провести сеанс связи, он автоматически получает доступ к любому свободному каналу. По окончании соединения канал может быть автоматически предоставлен другому.

1.Разновидности транкинговых систем

1.1 Без канала управления.

В этом случае свободный канал “помечается” специальным сигналом – маркером. Центральная станция такой системы периодически передает определенную последовательность, автоматически распознаваемую станцией абоненты. В случае вызова радиостанция занимает любой из свободных каналов. Все это происходит незаметно для пользователя – не нужно беспорядочно нажимать клавиши и прислушиваться к шумам эфира.

К таким системам относятся SmarTrunk II фирмы «SmarTrunk System inc.» и Larcer фирмы «CES».

Достоинства таких систем – это дешевое базовое и периферийное оборудование, простота установки и эксплуатации.

Недостатки этих систем:

1. при увеличении количества каналов и загрузки системы существенно увеличивается время поиска свободного радиоканала для установления связи;

2. время установления связи больше, чем у других систем;

3. невозможность создания многозоновых систем; сокращенный набор функций и сервиса.

1.2 Вторая разновидность транкинговых систем имеет канал управления. Присутствие его сводит к минимуму время ожидания соединения. В этом случае система сама определяет наличие незанятых каналов и переключает на них станцию абонента.

1.3 Система с выделенным каналом.

Многие крупнейшие компании используют при построении сети управление на основе выделенного канала.

Микропроцессорный блок управления контролирует все базовые станции в зоне обслуживания. Один из каналов выделяется для использования исключительно в целях правления и представляет собой своеобразное «руководящее звено» данной системы. Его основная функция – установления соединения между двумя абонентами сети.

К системам с выделенным каналом управления относятся SmartNet, SmartZone фирмы Motorola и все системы, построенные на основе протокола MPT 1327 – ACCESSNET, ActioNet, TaitNet.

У таких систем наличие выделенного канала управления увеличивает общее количество радиоканалов системы.

При использовании выделенного канала управления все запросы на доступ к системе осуществляются через этот канал. При этом максимальное использование ресурсов, обеспечиваемое методом ALOHA, применяемом в системах с выделенным каналом управления, составляет около 37%. В результате ресурсы системы ограничены даже при передаче по управляющему каналу коротких пакетов.

Система обрабатывает все поступающие запросы только последовательно. При увеличении загрузки и уменьшении числа свободных каналов время ожидания увеличивается экспоненциально.

1.4 Транкинговые системы без выделенного контрольного канала.

В системах такого рода в место специально выделенного канала используется один из приемопередатчиков центральной станции. За той или иной группой не жестко закрепляется один из каналов, который он не занял. В противном случае блок управления (контроллер), распределяющий каналы системы, переключает пользователя на любой свободный. Если заняты все каналы, аппарат сообщает об этом при попытке начать сеанс связи.

Постоянное обновление информации достигается посредством того, что не занятый в сеансе связи приемопередатчик и определенной частотой передает короткие пакеты данных закрепленным за ним мобильным устройствам и центральным станциям. Таким образом постоянно имеется информация о свободных на данный момент канала. Эти данные используются при автоматическом переключении устройств.

2. Построение транкинговых систем.

При построении крупных межрегиональных систем в транкинговых сетях может быть предусмотрена возможность роуминга, т.е. использование радиостанций в других пунктах.

2.1 Построение однозоновой системы

Первоначально транкинговые системы строились по однозоновому принципу, когда весь канальный ресурс закреплялся за одной центральной станцией. Антенна такой станции обычно располагалась по принципу маяка – в наиболее высокой точке предполагаемой зоны обслуживания.

Приемопередатчик каждого канала контролируется специальным блоком управления – контроллером. Максимальное число каналов на центральной станции – 24, причем один из них управляющий. Для приведения сеанса связи он предоставляет любой из свободных каналов системы. Общее взаимодействие системы осуществляется через блок сопряжения.

По общей шине передачи данных он соединен с контроллерами каналов, обеспечивая функциональное управление, учет и тарификацию соединений, а так же контроль ее состояния и конфигурацию через терминал управления SYSCON. Терминал может подключаться непосредственно через порт RS 232 или, если вы хотите заслужить репутацию прогрессивного молодого специалиста, по модему.

2.2 Построение многозоновой системы.

Строится путем объединения центральных станций. Ее сердце – центральный узел, на который возложены все функции управления. В состав узла входят центральный процессор и коммутатор разговорных каналов. При этом центральный процессор может управлять до 10 центральными станциями по обычным проводным линиям через порты RS 232. Коммутатор осуществляет соединение разговорных каналов в соответствии с командами, поступившими из центрального процессора.

Многозоновые системы могут иметь либо радиальную, либо линейную структуру.

2.3 Построение крупных межрегиональных систем.

Можно объединить через межрегиональный процессор до 16 систем MPT-1327, осуществляя коммуникацию разговорных каналов через дополнительный коммутатор.

Стандарт МРТ-1327 удовлетворяет всем основным требованием, предъявленным к стандартам подобного рода: он обеспечивает вам возможность широкого выбора аппаратного обеспечения различных производителей и объединение разразненных сетей в единую. Кроме того, системы, основанные на данном стандарте, не просто эффективны, но и выгодны экономически. Во многих системах предусмотрена проверка каждой радиостанций на право пользование связью при каждом вызове, что обеспечивает достаточно эффективную защиту информации.

Список использованных источников

1. Тамаркин В. "Транкинговые системы радиосвязи", Эко-Трендз, 1997 г.
2. Овчинников А. "Открытые стандарты цифровой транкинговой радиосвязи", Эко-Трендз, 2000 г.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Махаев Егор Геннадьевич, курсант 2-ого курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Информационные технологии являются составной частью научного направления «Информатика» и базируется на её достижениях. Но в настоящее время недостаточно владеть информацией, её необходимо применять и реализовывать. Эту задачу решают информационные технологии, основная цель которых – обработка информации различных видов.

На основе информационных технологий решается задача автоматизации информационных процессов. Информация, как продукт информационных технологий, структурируется и формируется в виде знаний.

Опыт внедрения информационных технологий подтверждает их высокую экономическую эффективность для многих сфер применения. Яркими примерами могут служить системы электронного документооборота и организация дистанционного обучения на базе современных телекоммуникационных и информационных технологий.

В данном учебном пособии рассматриваются основные теоретические положения информационных технологий, раскрываются базовые информационные технологии, такие как телекоммуникационные технологии и технологии искусственного интеллекта, приводятся различные интегрированные информационные технологии.

Возрастание объёма информации особенно стало заметно в середине XX в. Лавинообразный поток информации хлынул на человека, не давая ему возможности воспринять эту информацию в полной мере. В ежедневно появляющемся новом потоке информации ориентироваться становилось всё труднее. Подчас выгоднее стало создавать новый материальный или интеллектуальный продукт, нежели вести розыск аналога, сделанного ранее.

Как результат – наступает информационный кризис (взрыв), который имеет следующие проявления:

• появляются противоречия между ограниченными возможностями человека по восприятию и переработке информации и существующими мощными потоками и массивами хранящейся информации. Так, например, общая сумма знаний менялась вначале очень медленно, но уже с 1900 г. она удваивалась каждые 50 лет, к 1950 г. удвоение происходило каждые 10 лет, к 1970 г. – уже каждые 5 лет, с 1990 г. – ежегодно, а в наши дни – ещё быстрее;

• существует большое количество избыточной информации, которая затрудняет восприятие полезной для потребителя информации;

• возникают определённые экономические, политические и другие социальные барьеры, которые препятствуют распространению информации (например, введение грифа секретности или «для служебного пользования» для некоторого вида информации).

Эти причины породили весьма парадоксальную ситуацию – в мире накоплен громадный информационный потенциал, но люди не могут им воспользоваться в полном объёме в силу ограниченности своих возможностей. Информационный кризис поставил общество перед необходимостью поиска путей выхода из создавшегося положения. Внедрение современных средств переработки и передачи информации в различные сферы деятельности послужило началом нового эволюционного процесса в развитии человеческого общества, находящегося на этапе индустриального развития, который получил название информатизации

Список использованных источников

1. А.В.Майстеренко, Н.В.Майстеренко Информационные технологии в науке, Образовании и инженерной практике

ЗАЩИТА ОТ АТАК НА DHCP-СЕРВЕР

Михайлов Александр Сергеевич
Научный руководитель Поликарпов Евгений Сергеевич
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Общая характеристика службы DHCP.

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это протокол, который позволяет устройствам в сети автоматически получать сетевые параметры (в том числе и IP-адрес).

Клиент, настроенный на автоматическое получение IP-адреса отправляет широковещательные адреса сетевого (IP-адрес 255.255.255.255) и канального (MAC-адрес – FF:FF:FF:FF:FF:FF) уровней для обнаружения DHCP-серверов. Данный пакет получают все устройства в сети, но отвечает на него только DHCP-сервер. До получения IP-адреса от одного из возможных DHCP-серверов в поле адреса источника IP-пакета указывается IP-адрес 0.0.0.0, т.к. клиент еще не получил данный параметр. В поле источника сообщения на канальном уровне указывается MAC-адрес клиента. Такое сообщение называется «DHCPDISCOVER».

Если вдруг на данное сообщение клиента не ответил ни один DHCP-сервер в течении одной секунды, то клиент повторно отправляет запросы еще пять раз (интервал между запросами составляет приблизительно 30 сек). В случае, если ответ от сервера так и не получен, то клиент получает IP-адрес по технологии APIPA (Automatic Private IP Addressing) из диапазона от 169.254.0.1 по 169.254.255.254 с маской подсети 255.255.0.0.

После того, как любой из возможных DHCP-серверов получает широковещательное сообщение, описанное выше, он отправляет на MAC-адрес клиента пул предлагаемых IP-адресов. Данное сообщение, адресованное от сервера к клиенту, называется «DHCPOFFER». На время предложения данные IP-адреса резервируются DHCP-сервером и не предлагаются другим клиентам. Данные действия проделывают все DHCP-сервера, получившие широковещательное сообщение.

Предположим, что клиент получил сообщение «DHCPOFFER» от одного из DHCP-серверов. Тогда клиент отправляет широковещательное сообщение «DHCPREQUEST», в котором содержится IP-адрес сервера, выдавшего предложение. Такое широковещательное сообщение информирует другие DHCP-серверы о том, что клиент уже принял предложение от одного из серверов. В таком случае остальные DHCP-серверы освобождают зарезервированные IP-адреса и в дальнейшем они могут быть предложены другим клиентам.

После получения сервером сообщения «DHCPREQUEST» он вносит выбранный клиентом IP-адрес в определенное поле сообщения «DHCPACK». После получения подтверждения клиент полностью инициализирует протокол TCP/IP на своем сетевом интерфейсе.

Виды атак на DHCP-сервер.

Существует два основных вида атак на DHCP-сервер: DHCP Starvation и Rogue DHCP. Принцип работы DHCP Starvation в следующем: генерируется большое количество сообщений типа «DHCPDISCOVER» с запросом аренды IP-адреса на широковещательные адреса сетевого и канального уровней, на порт назначения – 67, т.е. на DHCP-сервер. При этом MAC-адрес источника каждый раз изменяется на новый. Соответственно, DHCP-сервер, получая такие сообщения, резервирует IP-адреса из пула, что и приводит к отказу в обслуживании легитимных клиентов, желающих арендовать IP-адрес для выхода в сеть.

Rogue – от англ. мошенник. Атака Rogue DHCP является видом атаки типа Man in the Middle (человек посредине). Суть этой атаки заключается в развертывании поддельного DHCP-сервера, который в свою очередь будет предоставлять аренду клиентам поддельные сетевые параметры, а именно – адрес шлюза. В качестве адреса шлюза выступает IP-адрес атакующей машины. Таким образом, сетевой трафик, отправляемый клиентами в удаленные

сети, будет проходить через шлюз по умолчанию (атакующую машину), что позволит «прослушивать» трафик ничего не подозревающих клиентов.

Защита от атак на DHCP-сервер на примере сетевого оборудования Cisco.

Предотвратить атаку типа DHCP Starvation можно с помощью функции безопасности порта коммутатора Cisco. Работа этой функции заключается в ограничении количества допустимых MAC-адресов на определенном порту коммутатора, которым доступ разрешен.

Что касается атаки Rogue DHCP, то предотвратить ее можно также с помощью функции безопасности коммутаторов. Для этого коммутатор настраивается функцией DHCP Snooping, с помощью которой он отбрасывает DHCP-пакет (а именно сообщения, адресованные от сервера клиенту: DHCPOFFER, DHCPACK, DHCPNACK), который пришел на ненадежный порт. Тем самым становится невозможным развертывание поддельного DHCP-сервера, так как коммутатор будет просто отбрасывать его пакеты.

Также, необходимо не забывать о ведении журнала службы DHCP. При расследовании инцидентов источником доказательственной базы могут служить системные события службы DHCP. К примеру, изучив логи DHCP-сервера в сети можно выяснить в какой промежуток времени устройство с определенным физическим адресом владело некоторым арендованным IP-адресом.

СПОСОБЫ ВЫЯВЛЕНИЯ УЯЗВИМОСТЕЙ ПРИКЛАДНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Молчков Григорий Романович, командир отделения, сержант полиции
Научный руководитель Плотников Герман Геннадьевич, профессор, кандидат технических наук, полковник полиции
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Ключевые слова: программное обеспечение, уязвимости, методы.

Аннотация:

Статья приводит методы и способы обнаружения уязвимостей и анализ угроз прикладного программного обеспечения.

Любой компьютер или сервер нуждается, для полноценного функционирования, не только в качественном аппаратном обеспечении, но и в не менее качественном, а главное, безопасном программном обеспечении. Уязвимость программного обеспечения может рассматриваться как недостаток, слабость или даже ошибка в системе, которая может быть использована злоумышленником для изменения нормального поведения системы. Потому что количество программных систем увеличивается с каждым днем и количество уязвимостей вместе с ними. Кроме того, если учесть, что большинство систем используются несколькими пользователями (в сети Интернет) и различными средами (например, операционными системами), то это просто вопрос времени, когда кто-то может начать атаку, последствия которой непредсказуемы в плане ущерба.

Обычно целью злоумышленника является получение некоторых привилегий в системе для получения контроля над ним или получения ценной информации для его собственной выгоды. Тогда разработчикам и широкой общественности важно знать об возможных уязвимостях, их предотвращении и обнаружении.

Для лучшего понимания уязвимостей очень полезно создание моделей, выражающих заданные условия, которые могут привести к их возникновению или создать их; Кроме того, когда модели хорошо понятны, их также можно использовать для профилактики. Но поскольку невозможно гарантировать отсутствие уязвимостей в фрагменте кода при его создании, то необходимо иметь методы для их обнаружения. Одной из возможностей является проверка программного обеспечения безопасности или просто ручная проверка кода или связанных документов. Также могут быть применены некоторые более автоматизированные методы обнаружения уязвимостей, которые подразделяются на две основные категории: статические, когда обнаружение выполняется без запуска исходного кода; и динамический, когда программа выполняется для обнаружения уязвимостей [1].

Как уже было сказано выше, злоумышленники могут использовать уязвимую программную систему, и взломать ее. Злоумышленник может взять под контроль систему, чтобы повредить ее, запустить новые атаки или получить некоторую конфиденциальную информацию, которую он может использовать для своей собственной выгоды. Учитывая это, важно знать различные типы уязвимостей, их предотвращение и обнаружение, чтобы попытаться избежать их присутствия в окончательной версии программного обеспечения системы, а затем уменьшить вероятность атак и серьезных повреждений.

Большинство известных уязвимостей связаны с неправильным способом обработки входных данных, предоставленных пользователем системы, если эти входные данные не обрабатываются правильно перед использованием их внутри программы, они могут вызвать непредвиденное поведение системы. Чаще всего уязвимости единственные в своем роде, и максимально отличаются от остальных, вне зависимости от степени угрозы, поэтому провести систематизацию их или бессмысленно или невозможно. Грамотно классифицировать их можно следующим образом [2]:

- Уязвимости и угрозы возникшие в момент создания и проектирования программного обеспечения;

- Уязвимости в ходе эксплуатации;
- Уязвимости в процессе внесения координирующих дополнений, обновлений, конфигураций.

Переходя ближе к самим способам и методам обнаружения, можно сказать, что построение моделей, тестирование и анализ максимально полезны для понимания и предотвращения данных уязвимостей; тем не менее, необходимо также рассчитывать на инструменты, которые могут использовать программисты для выявления уязвимостей в процессе создания программного обеспечения.

Некоторые из этих инструментов основаны на статических методах, поэтому нет необходимости запускать код для выполнения обнаружения. В случае динамических методов код запускается в контролируемой среде, чтобы выполнить обнаружение или собрать следы программы, которые можно использовать для этой цели. В следующем разделе мы представим некоторые статические и динамические методы для обнаружения уязвимостей [1].

Статические методы - это те, которые применяются непосредственно к исходному коду без запуска приложения, цель состоит в том, чтобы оценить или получить конкретную информацию непосредственно из исходного кода, не выполняя ее. Существуют разные методы для выполнения статического анализа [3]:

Сопоставление с образцом. Метод состоит в поиске строки «шаблона» в исходном коде и в качестве результата дает количество вхождений в нее.

Лексический анализ. Этот анализ добавляет дополнительный шаг перед применением сопоставления с образцом. Фактически исходный код преобразуется в последовательность «токенов», которые впоследствии сравниваются с базой данных уязвимостей для их идентификации. Количество ложных срабатываний все еще велико, поскольку они не учитывают синтаксис или грамматику программы.

Разбор. Синтаксический анализ является более сложным, чем лексический анализ, поэтому, когда исходный код анализируется, представление программы строится с использованием дерева синтаксического анализа для анализа синтаксиса и семантики программы. Например, метод синтаксического анализа используется для обнаружения атак внедрения SQL-команд.

Классификатор типа. Спецификаторы типов используются для определения типов и изменения свойств переменных в языке программирования.

Анализ потока данных. Цель состоит в том, чтобы определить возможные значения, которые может иметь переменная или выражение во время выполнения программы, особенно подходящие для обнаружения переполнения буфера. Процесс выполняется в трех частях: сопоставление с образцом, управление потоком данных и анализатор потока.

Анализ порчи. Особый случай анализа потока данных, когда любые данные, поступающие из ненадежных источников, например, введенные пользователем, представляют потенциальную проблему для системы, поэтому они помечаются как испорченные. Загрязненный поток данных отслеживается, поскольку он не может достичь критических функций, если он не обработан и не изменен на неиспользованный.

Проверка модели. Этот метод автоматического тестирования соответствия модели системы ее спецификации и ее можно использовать для обнаружения уязвимостей. Обычно проверка модели является сложной техникой, поскольку разработка модели затруднена, однако, как только она будет получена, ее проще будет проверить свойства системы.

Анализ ограничений объединяется с проверкой модели для выявления уязвимостей переполнения буфера. Они отслеживают объем памяти связанных с буфером переменных и кода, снабженного утверждениями об ограничениях перед потенциальными уязвимыми точками. Уязвимость может быть обнаружена с помощью способности подтверждения утверждения с помощью проверки модели.

Для динамического обнаружения уязвимостей необходимо выполнить программный код, а затем проанализировать поведение или ответы системы и вынести вердикт. Далее мы изучим некоторые методы для динамического обнаружения [3].

Ввод неисправности. Внедрение неисправности - это метод тестирования, который вводит неисправности для проверки поведения системы, для генерирования возможных неисправностей требуются определенные знания о системе. При обнаружении неисправностей можно обнаружить недостатки безопасности в системе, в процессе чего неисправности внедряются в тестируемую систему и наблюдается поведение системы, неспособность допустить неисправности является индикатором потенциальной уязвимости системы безопасности. Модель используется, чтобы решить, какие ошибки вводить.

Нечеткое тестирование. Идея этого теста заключается в предоставлении случайных данных в качестве входных данных для приложения, чтобы определить, может ли приложение обрабатывать их правильно. Нечеткое тестирование легче осуществить, чем введение ошибки, потому что дизайн теста проще, и не всегда требуются предварительные знания о тестируемой системе, кроме того, оно ограничено точками входа в программу. Веб-сканеры находятся в этой категории инструментов.

Динамическое заражение. Этот метод аналогично с анализом заражения, но в этом случае испорченные данные отслеживаются во время выполнения программы, чтобы определить правильность их проверки перед вводом чувствительных функций. Это позволяет обнаруживать возможные проблемы проверки входных данных, которые считаются уязвимостями.

Санитарная обработка. Одной из возможностей избежать уязвимостей из-за использования пользовательских данных является реализация новых встроенных функций или пользовательских подпрограмм, основная идея которых заключается в проверке или дезинфекции любого ввода от пользователей перед использованием его внутри программы.

Проблема уязвимостей в прикладном программном обеспечении не теряет своей актуальности по сей день. Не стоит забывать, что пока выпускается новое программное обеспечение, появляются и новые уязвимости. Разработчикам и программистам следует тщательнее и внимательнее подходить к созданию новых утилит, приложений и инструментов. А специалистам в области информационной безопасности своевременно тестировать и анализировать готовое программное обеспечение в целях устранения возможных уязвимостей. Огромный риск состоит в том, что такие недоработки и ошибки приложений можно порой использовать для кражи информации разного уровня.

Список использованных источников

1. D. Byers, S. Ardi, N. Shahmehri, C. Duma. Modeling Software Vulnerabilities with Vulnerability Cause Graphs (Моделирование уязвимостей программного обеспечения с помощью графиков причин уязвимости). In Proceedings of the International Conference on Soft Maintenance, Philadelphia, PA, USA, – 2006.– С. 276–298

2. S. Christey. Unforgivable Vulnerabilities (Непростительная уязвимость). The MITRE Corpotarion. – 2007. – С. 9–18

3. Защита программного обеспечения / Под ред. Д. Гроувера; Пер. с англ. В.Г. Потемкина и др.; – М.: Мир, 1992. – 288 С. – 34–50.

РАЗРАБОТКА ИГРЫ С ЦЕЛЬЮ ЗНАКОМСТВА С ПРОМЫШЛЕННЫМ ПРЕДПРИЯТИЕМ И РАБОЧИМИ ПРОФЕССИЯМИ ПРИ ПОМОЩИ МУЛЬТИМЕДИЙНЫХ СРЕДСТВ И ГЕЙМИФИКАЦИИ: «ПРИКЛЮЧЕНИЯ МЕТАЛЛУРГА В АО «УРАЛЭЛЕКТРОМЕДЬ» – ПУТЕШЕСТВИЕ ПО ЦЕХАМ ПРЕДПРИЯТИЯ»

Мориков Данил Александрович, Рябцев Сергей Викторович
Научный руководитель Клепикова Екатерина Дмитриевна, преподаватель
ГАПОУ СО «УГК им. И.И. Ползунова», г. Екатеринбург

Актуальность. Знакомство школьников и студентов с промышленным предприятием, рабочими профессиями (а также производственная практика для студентов) является важным средством профориентации и трудового воспитания.

Одним из актуальных направлений развития образовательных технологий является геймификация.

Геймификация – технология использования игровых методов в неигровом контексте, в том числе в управлении рабочим персоналом и оборудованием. Геймификация может стать отличным инструментом мотивации, вовлечения и адаптации школьников и студентов на предприятии.

Внедрение игровых элементов в процесс выбора будущей профессии и прохождения производственной практики способствует более прочному усвоению научных основ производства и получения профессиональных навыков.

Проблема. Необходимо разработать онлайн-экскурсию – знакомство с промышленным предприятием (АО «Уралэлектромедь»), рассмотреть востребованные рабочие профессии и технические процессы на предприятии с помощью мультимедийных средств и геймификации, познакомить дистанционно школьников и студентов с предприятием (в игровой форме).

Разработанность исследуемой проблемы. Проанализировав доступные нам источники информации и пообщавшись со студентами-практикантами, мы можем отметить следующее: внедряемый проект способствует повышению интереса к востребованным профессиям среди школьников и студентов – экскурсантов, знакомит с производством и рабочим процессом, техникой безопасности, помогает экскурсантам определиться с дальнейшей профессиональной деятельностью.

Наглядное (зрительное) восприятие технологического процесса формирует у школьников и студентов представление о деятельности АО «Уралэлектромедь», способствует получению новых знаний и профессиональных навыков.

Цель. Разработать игровое приложение с целью знакомства с промышленным предприятием (АО «Уралэлектромедь») и рабочими профессиями (в удаленном формате) при помощи мультимедийных средств и геймификации.

Задачи.

- познакомиться с рабочими профессиями и деятельностью АО «Уралэлектромедь»;
- познакомиться с методами разработки игровых приложений и инструментальными средами;
- выбрать инструментальные средства для создания игрового приложения;
- разработать концепцию игрового приложения;
- создать макеты персонажей, сцен, игровые моменты;
- разработать программный код;
- создать удобный пользовательский интерфейс;
- отладить и протестировать разработанное игровое приложение;
- составить программную документацию.

Среди множества методов и форм обучения экскурсия занимает прочные позиции в технологической подготовке обучающихся. Это связано с ее неоспоримыми преимуществами, главным из которых является включенность обучающегося в процесс

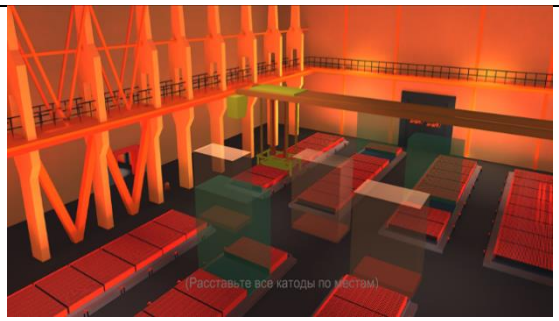
познания, непосредственное наблюдение за технологическими процессами, функционированием технологического оборудования, профессиональной деятельностью людей различных профессий в АО «Уралэлектромедь». Но среди преимуществ экскурсии есть ее значительный недостаток – ресурсоемкость. Для организации и проведения экскурсии необходимо затратить время на подготовку документов и согласований.

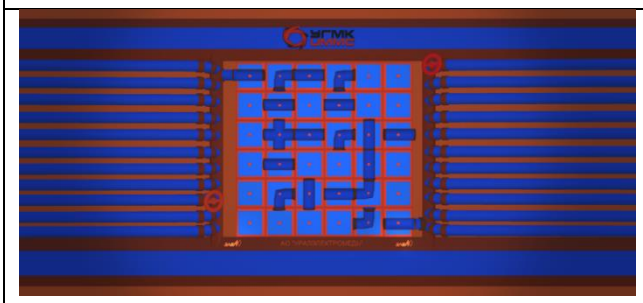
Наша виртуальная экскурсия-видеоигра – это форма обучения, сочетающая рассказ робота-помощника с демонстрацией наглядного материала и применением игровых элементов.

После успешного прослушивания экскурсии и прохождения всех мини-игр, появится обучающий тест с вопросами для проверки и укрепления пройдённого материала, где необходимо выбрать правильные варианты ответов. Результатом является пройденный тест на «отлично», если результат является «неудовлетворительным», можно вернуться к началу онлайн-экскурсии (игры) и пройти её заново.

Для технологической подготовки обучающихся виртуальная экскурсия-игра открывает очень большие возможности. Так, например, можно наблюдать за такими технологическими процессами, которые недоступны для наблюдения в реальности. Обучающиеся получают возможность побывать в цехах предприятия, не выходя из классной комнаты.

Виртуальная экскурсия-видеоигра обладает высоким профориентационным потенциалом, позволяет наглядно познакомиться с различными профессиями и увидеть производственный процесс.





Создание видеоигры (виртуальной экскурсии по цеху) имеет положительный профориентационный эффект, который поможет школьникам определиться с профессиональным выбором, а студентам-целевикам – адаптироваться к производственным условиям, закрепить полученные знания и подготовиться к прохождению производственных

практик в реальных условиях. Во время экскурсий на производство школьники и студенты познакомятся с работой предприятия, востребованными профессиями, основами производства, технологическим процессом, что будет способствовать формированию у них правильного представления о деятельности АО «Уралэлектромедь» и получению новых знаний, профессиональных навыков. Проект актуален для подготовки будущих высококвалифицированных рабочих.

Данный проект принесет для предприятия еще и экономический эффект, так как виртуальная экскурсия по цеху позволит сэкономить финансовые ресурсы, направленные на оплату специалистам, сопровождающим экскурсию, а также – на оплату автобуса (доставка до цеха на автобусе – это требование по технике безопасности).

Заработная плата одного специалиста, сопровождающего экскурсию, составляет 200 рублей в час. На одну экскурсию требуется 2-3 сопровождающих лица. Налог от суммы составляет 31,9 рублей. Стоимость автобуса: 1272 рубля за 1 час.

За 2019 год на организацию и проведение экскурсий было израсходовано: на заработную плату – 29806 рублей, на налог – 9506 рублей, на оплату автобуса – 103960 рублей.

Итого: оценка экономической эффективности внедрения проекта составляет 143 тысячи 272 рубля.

Подводя итоги, мы можем с уверенностью сказать, что добились своей цели.

Онлайн-экскурсии в игровом приложении являются отличным способом стимулирования школьников к выбору будущей профессии, а студентов – к обучению.

Актуальность онлайн-экскурсий в игровом формате не вызывает никаких сомнений, и заключается в подготовке будущих специалистов, в формировании их умений и навыков, решении кадрового вопроса.

Игровое приложение действительно конкретизирует уже имеющиеся профессиональные знания, способствует формированию новых, показывает востребованность профессиональных умений.

Чередование онлайн-экскурсии с теоретическими знаниями позволит достичь высоких результатов при освоении основной профессиональной образовательной программы в соответствии с ФГОС.

Во время прохождения игры-экскурсии оказывается целенаправленное воздействие на мотивационную сферу школьников и студентов:

- появляется интерес к деятельности, развивается или стимулируется любознательность;
- экскурсия-игра строится по принципу сотрудничества, взаимодействия и поддержки, а это значит – каждый экскурсант видит свою ценность и уникальность;
- вовремя онлайн-экскурсии экскурсант учится планировать свою деятельность, определять цель и предвидеть результат;
- экскурсант учится объяснять и вникать в суть происходящего;

Методика проведения экскурсий в игровом приложении направлена на то, чтобы помочь школьникам и студентам легче усвоить теоретический материал и удаленно познакомиться с АО «Уралэлектромедь».

Список использованных источников

1 https://elem.ru/ru/

2 www.game-maker.ru -- создание игр. Огромный выбор примеров, исходников, уроков, статей, игр созданных на Game Maker. А также новости, конкурсы, книги, журналы из мира GM.

3 Unity в действии. Мультиплатформенная разработка на C#. - М.: Питер, 2018. - 608 с.

4 Язык программирования C#. Классика Computers Science. 4-е изд. Авторы: А. Хейлсберг, М. Торгерсен, С. Вилтамут, П. Голд

5 https://docs.unity3d.com/ru/530/ScriptReference/

ОСНОВНАЯ ОПЕРАЦИОННАЯ СИСТЕМА В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Мосин Андрей Алексеевич, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Linux — семейство операционных систем с открытым исходным кодом. Это значит, они могут модифицироваться (изменяться) и распространятся любым человеком по всему миру. Это очень отличает эту ОС от других, таких как Windows, которая может изменяться и распространяться только самим владельцем (Microsoft). Преимущества Линукса в том, что он бесплатный, и есть много различных версий на выбор.

Наиболее популярные операционные системы линейки Linux :

Ubuntu

Ubuntu - это операционная система с открытым исходным кодом, основанная на дистрибутиве Debian GNU / Linux.

Ubuntu включает в себя все функции ОС Unix с добавленным настраиваемым графическим интерфейсом, что делает его популярным в университетах и исследовательских организациях. Ubuntu в первую очередь предназначен для использования на персональных компьютерах, хотя серверные версии также существуют.

Впервые Ubuntu была выпущена в 2004 году. Проект спонсируется компанией Canonical Ltd., базирующейся в Великобритании, которая получает доход, продавая поддержку и услуги в дополнение к Ubuntu. Canonical выпускает новую версию Ubuntu каждые шесть месяцев и обеспечивает поддержку в виде исправлений и выпусков безопасности в течение 18 месяцев после этого.

Ubuntu состоит из множества программных пакетов, которые лицензируются в соответствии с GNU General Public License. Это позволяет пользователям копировать, изменять, разрабатывать и распространять свои собственные версии программы.

Ubuntu поставляется с широким спектром программ, включая FireFox и LibreOffice. Есть также проприетарное программное обеспечение, которое можно запускать в Ubuntu.

Debian

Debian, также известный как Debian GNU / Linux, представляет собой дистрибутив Linux, состоящий из бесплатного программного обеспечения с открытым исходным кодом, разработанного поддерживаемым сообществом проектом Debian, который был создан Ианом Мердоком 16 августа 1993 года. Первая версия Debian (0.01) был выпущен 15 сентября 1993 года, а его первая стабильная версия (1.1) была выпущена 17 июня 1996 года. Ветка Debian Stable является наиболее популярной версией для персональных компьютеров и серверов. Debian также является основой для многих других дистрибутивов, особенно Ubuntu.

Debian является одной из старейших операционных систем на основе ядра Linux. Проект координируется через Интернет командой добровольцев под руководством Лидера Проекта Debian и трех основополагающих документов: Социальный договор Debian, Конституция Debian и Руководства по бесплатному программному обеспечению Debian. Новые дистрибутивы постоянно обновляются, а следующий кандидат освобождается после временной остановки.

С момента своего основания Debian разрабатывался открыто и распространялся свободно в соответствии с принципами проекта GNU. В связи с этим Фонд свободного программного обеспечения спонсировал проект с ноября 1994 года по ноябрь 1995 года. Когда спонсорство прекратилось, проект Debian создал некоммерческую организацию Software in the Public Interest для продолжения финансовой поддержки развития.

Mint

Linux Mint - это бесплатный дистрибутив операционной системы с открытым исходным кодом (ОС), основанный на Ubuntu и Debian, для использования на машинах, совместимых с x-86 x-64.

Mint разработан для простоты использования и готового к использованию интерфейса, включая поддержку мультимедиа на настольных ПК. Операционная система проще в установке, чем большинство дистрибутивов Linux. Mint включает в себя программное обеспечение, необходимое для электронной почты и онлайн-функций, а также поддержку мультимедийного контента, будь то онлайн или из собственных файлов пользователя и физических носителей.

В отличие от большинства дистрибутивов Linux, Mint включает в себя собственные сторонние плагины для браузеров, Java, медиа-кодеки и другие компоненты, обеспечивающие поддержку общепринятых стандартов. Эта поддержка позволяет воспроизводить DVD и BluRay, а также Flash для потоковой передачи мультимедиа. Хотя операционная система включает в себя брандмауэр, Mint утверждает, что не нуждается в вредоносных программах. Mint совместим с установщиком Ubuntu, который обеспечивает доступ к 30 000 существующих бесплатных программ с открытым исходным кодом.

Существует несколько различных версий Mint для настольных компьютеров, включая Cinnamon, GNOME, XFCE и KDE, для лучшей поддержки различного оборудования. Операционная система также предоставляется в альтернативном выпуске Linux Mint Debian Edition для тех, кто более знаком с Linux. Это издание считается менее интуитивным и удобным для пользователя, но также более быстрым и более отзывчивым.

Linux Mint является третьей по популярности домашней операционной системой после Windows от Microsoft и Mac OS от Apple.

Он работает из коробки, с полной поддержкой мультимедиа и чрезвычайно прост в использовании.

Он бесплатен и с открытым исходным кодом.

Основанный на Debian и Ubuntu, он предоставляет около 30 000 пакетов и одного из лучших менеджеров программного обеспечения.

Это безопасно и надежно. Благодаря консервативному подходу к обновлениям программного обеспечения, уникальному диспетчеру обновлений и надежности своей архитектуры Linux, Linux Mint требует минимального обслуживания (без регрессии, без антивируса, без антишпионского ПО и т. Д.).

Kali Linux

Kali Linux - это дистрибутив Linux на основе Debian, предназначенный для расширенного тестирования на проникновение и аудита безопасности. Kali содержит несколько сотен инструментов, предназначенных для решения различных задач информационной безопасности, таких как тестирование на проникновение, исследование безопасности, компьютерная криминалистика и обратный инжиниринг. Kali Linux разрабатывается, финансируется и поддерживается Offensive Security, ведущей компанией по обучению информационной безопасности.

Kali Linux был выпущен 13 марта 2013 года как полная перестроенная версия BackTrack Linux, полностью соответствующая стандартам разработки Debian.

Включено более 600 инструментов для тестирования на проникновение. Изучив каждый инструмент, включенный в BackTrack, мы исключили большое количество инструментов, которые либо просто не работали, либо дублировали другие инструменты, которые обеспечивали такую же или аналогичную функциональность. Подробная информация о том, что включено, находится на сайте Kali Tools.

Бесплатно (как в пиве) и всегда будет: Kali Linux, как и BackTrack, полностью бесплатен и всегда будет. Вам никогда не придется платить за Kali Linux.

Дерево Git с открытым исходным кодом: Мы привержены модели разработки с открытым исходным кодом, и наше дерево разработки доступно для всеобщего обозрения. Весь исходный код, который входит в Kali Linux, доступен для всех, кто хочет настроить или перестроить пакеты в соответствии с их конкретными потребностями.

Соответствует FHS: Kali придерживается стандарта иерархии файловых систем, что позволяет пользователям Linux легко находить двоичные файлы, файлы поддержки, библиотеки и т. Д.

Широкая поддержка беспроводных устройств: для беспроводных интерфейсов поддерживается стандартная точка отсчета в дистрибутивах Linux.

Kali Linux создали для поддержки как можно большего количества беспроводных устройств, что позволяет ему правильно работать на широком спектре оборудования и делает его совместимым с многочисленными USB и другими беспроводными устройствами.

Кастомное ядро, исправленное для инъекций. В качестве тестеров на проникновение команде разработчиков часто нужно проводить беспроводные оценки, поэтому в ядро включены самые последние патчи для внедрения.

Разработано в защищенной среде. Команда KaliLinux состоит из небольшой группы людей, которым доверяют только фиксацию пакетов и взаимодействие с репозиториями, причем все это выполняется с использованием нескольких безопасных протоколов.

Подписанные GPG пакеты и репозитории: каждый пакет в Kali Linux подписывается каждым отдельным разработчиком, который его создал и зафиксировал, и впоследствии репозитории также подписывают пакеты.

Многоязыковая поддержка: хотя инструменты проникновения написаны на английском языке, Kalівключет настоящую многоязычную поддержку, позволяющую большему количеству пользователей работать на своем родном языке и находить инструменты, необходимые для работы.

Полностью настраиваемый: для более предприимчивых пользователей как можно проще настроить Kali Linux по своему вкусу вплоть до самого ядра.

Поддержка ARMEL и ARMHF: поскольку одноплатные системы на базе ARM, такие как Raspberry Pi и BeagleBone Black, среди прочего, становятся все более распространенными и недорогими, мы знали, что поддержка Kali ARMдолжна быть настолько надежной, насколько разработчики смогут обеспечить, с полностью работающими установками для систем ARMEL и ARMHF. Kali Linux доступен на широком спектре устройств ARM и имеет репозитории ARM, интегрированные с основным дистрибутивом, поэтому инструменты для ARM обновляются вместе с остальной частью дистрибутива.

ИСПОЛЬЗОВАНИЕ ОРГАНАМИ ВНУТРЕННИХ ДЕЛ ИНСТРУМЕНТОВ ПО РАБОТЕ С BIG DATA

Мурашев Андрей Евгеньевич, студент 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Современное общество неслучайно называют информационным. Человек — главный генератор и потребитель информации. Ежедневно мы создаем столько новой информации, на создание которой раньше уходили десятилетия. Эта информация является неструктурированной и абсолютно разнородной. По подсчётам учёных, 90% из существующей на данный момент информации было создано в течении последних двух лет. Так, посредством одного из поисковиков - Google совершается приблизительно 40 000 поисковых запросов каждую секунду, что приводит к 1,2 триллиону поисковых запросов ежегодно.

В связи с отсутствием структурированности информации и разрозненности данных о каждом человеке, данная информация очень сильно теряет в пригодности к использованию и ценности. Большие объёмы информации, которые получают из различных источников, в том числе и из сети Интернет принято называть Большими данными (Big Data).

Впервые понятие "Большие данные (Big Data)" было использовано Клиффордом Линчем и опубликовано в журнале Nature в сентябре 2008 года. Изначально данный термин использовался в научной среде, однако с 2009 года этот термин стали применять в коммерческо-деловой прессе, а к 2010 году появляются первые программно - аппаратные продукты и решения, непосредственно выполняющие функции по обработки больших данных. В 2011 году компания Gartner выделила Большие данные как второй тренд в инфраструктуре информационных технологий. Популярнее были только виртуализаци, энергосбережение и мониторинг. Согласно прогнозам, внедрение технологий больших данных сможет оказать наибольшее влияние на информационные технологии в сфере производства, торговли, здравоохранения, государственного управления, и других. С 2013 в рамках дисциплины «наука о данных» начали изучаться Большие данные.

Использование Big Data происходит и в ОВД, где есть возможность сбора разнородной информации из большого количества как открытых, так и закрытых источников. Собранная информация систематизируется и объединяется по различным признакам, сводится в базы данных и реестры, что позволяет не только использовать её в оперативных целях, но и осуществлять прогнозирование преступных действий. Так, например, статистическая информация об уровне преступности, о месте, времени, типе и числе пострадавших от различных преступных посягательств позволяет наиболее оптимально определить количества выделяемых для решения оперативных задач сил и средств. Также на основе социальных данных, полученных из различных источников, можно прогнозировать совершение преступных деяний, если сотрудниками была получена информация о фактах домашнего насилия в отдельных семьях.

Развитие информационных технологий в сфере охраны порядка также требует повышения внимания к качеству данных, на основе которых делаются прогнозы. Данные могут быть взяты из источников разного уровня и иметь большую качественную дифференциацию. Изъяны в обрабатываемой информации могут приводить к погрешностям анализа, которые в свою очередь оборачиваются весьма серьезными последствиями, когда дело доходит до судебного преследования.

Таким образом, было бы ошибкой считать Big Data не перспективным направлением, ведь именно оно позволяет решить проблему не только раскрытия преступлений, но и прогнозирования, а, следовательно, предотвращения совершения преступлений с использованием механизмов обработки и аналитики большого количества собранной информации. Перспективность и широкая вариативность применения инструментов по

структурированию и анализу Big Data для решения задач по борьбе с преступностью сложно переоценить даже с учетом того, что, как уже было отмечено раннее, основной проблемой использования Больших данных в настоящее время является плохая систематизация получаемых сведений, их большой объем, для обработки которого требуется разработка и внедрение новых либо оптимизация уже существующих аппаратно-программных комплексов и решений.

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ ВЫЧИСЛИТЕЛЬНЫХ СЕТЯХ, ПОСТРОЕННЫХ НА БАЗЕ ОБОРУДОВАНИЯ ФИРМЫ CISCO

Мыщик Алексей Юрьевич, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Задача обеспечения безопасности является главной для Cisco, а главная проблема её заказчиков – это угроза той же безопасности.

Для защиты организации нужна соответствующая архитектура безопасности и постоянная бдительность, т.к. хакерство в настоящее время превратилось в полноценный бизнес, направленный на огромную прибыль

Хакеры стали очень организованными, они действуют с размахом и масштабы их вредоносной деятельности только растут. Подготовка атак ведётся продуманно и профессионально, они имеют хорошее финансирование и в будущем атак станет намного больше.

Сейчас цепочка атаки представляет собой не просто отдельные атаки, а целую теневую индустрию, которая поставила на конвеер кражу конфиденциальных данных для их дальнейшей продажи либо незаконного использования с целью обогащения.

Так что же делать до обнаружения атаки, во время атаки и после неё? Как заявляют представители cisco, при любом сценарии развития атаки и любых последствиях, они предоставляют все необходимые инструменты для успешной борьбы с кибератакой и защиты от неё на всех этапах. Модель, ориентированная на защиту от угроз - это лучшее решение для борьбы с киберзлом, которое ежедневно угрожает безопасности организаций.

Технологии фирмы Cisco Systems широко используются для построения защищенных компьютерных сетей. Аппаратно-программные комплексы Cisco можно встретить в сетях практически любых организаций. Соответственно, растет потребность в специалистах, способных не только эксплуатировать данное оборудование, но и разрабатывать на его базе сложные защищенные сетевые проекты, а также осуществлять анализ информационной безопасности таких сетей. Известно, что подобные специалисты весьма ценятся и могут рассчитывать на высокооплачиваемую работу.

Первая глава посвящена средствам обеспечения безопасности периметра сети – использованию статических и динамических списков доступа, применению межсетевых экранов Cisco PIX, созданию защищенного канала связи.

Вторая и третья главы посвящены обнаружению сетевых компьютерных атак. В них рассматривается технология обнаружения сетевых компьютерных атак на примере комплексов Cisco IDS Sensor и Cisco MARS.

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ФИРМЫ CISCO

Списки управления доступом

Стандартные списки доступа

Списки доступа (access lists) представляют собой общие критерии отбора, которые можно впоследствии применять при фильтрации дейтаграмм, для отбора маршрутов, определения приоритетного трафика и в других задачах. Списки доступа, производящие отбор по IP-адресам, создаются командами access-list в режиме глобальной конфигурации, каждый список определяется номером – числом в диапазоне от 0 до 99. Каждая такая команда добавляет новый критерий отбора в список.

IP-адрес и маска шаблона записываются в десятично-точечной нотации, при этом в маске шаблона устанавливаются биты, значение которых в адресе следует игнорировать, остальные биты сбрасываются. При этом сетевая маска (netmask) и маска шаблона (wildcard)

– это разные вещи. Например, чтобы строка списка сработала для всех узлов с адресами 1.16.124.xxx, адрес должен быть 1.16.124.0, а маска – 0.0.0.255, поскольку значения первых 24 бит жестко заданы, а значения последних 8 бит могут быть любыми. Как видно в этом случае маска шаблона является инверсией соответствующей сетевой маски. Однако маска шаблона в общем случае не связана с сетевой маской и даже может быть разрывной (содержать чередования нулей и единиц). Например, строка списка должна сработать для всех нечетных адресов в сети 1.2.3.0/24. Соответствующая комбинация адреса и маски шаблона: 1.2.3.1 0.0.0.254.

Комбинация «адрес-маска шаблона» вида 0.0.0.0 255.255.255.255 (то есть соответствующая всем возможным адресам) может быть записана в виде одного ключевого слова any. Если маска отсутствует, то речь идет об IP-адресе одного узла.

Операторы permit и deny определяют, соответственно, положительное (принять, пропустить, отправить, отобрать) или отрицательное (отбросить, отказать, игнорировать) будет принято решение при срабатывании данного критерия отбора. Например, если список используется при фильтрации дейтаграмм по адресу источника, то эти операторы определяют, пропустить или отбросить дейтаграмму, адрес источника которой удовлетворяет комбинации «адрес – маска шаблона». Если же список применяется для идентификации какой-либо категории трафика, то оператор allow отбирает трафик в эту категорию, а deny – нет.

Список доступа представляет собой последовательность из одного и более критериев отбора, имеющих одинаковый номер списка. Последовательность критериев имеет значение: маршрутизатор просматривает их по порядку; срабатывает первый критерий, в котором обнаружено соответствие образцу; оставшаяся часть списка игнорируется. Любые новые критерии добавляются только в конец списка. Удалить критерий нельзя, можно удалить только весь список. В конце списка неявно подразумевается критерий «отказать в любом случае» (deny any) – он срабатывает, если ни одного соответствия обнаружено не было.

Для аннулирования списка доступа следует ввести команду: **router(config)#no access-list <номер списка>.**

Чтобы применить список доступа для фильтрации пакетов, проходящих через определенный интерфейс, нужно в режиме конфигурации этого интерфейса ввести команду:

router (config-if)#ip access-group <номер_списка> <{in/out}>.

Ключевое слово in или out определяет, будет ли список применяться к входящим или исходящим пакетам соответственно. Входящими считаются пакеты, поступающие к интерфейсу из сети. Исходящие пакеты движутся в обратном направлении.

Только один список доступа может быть применен на конкретном интерфейсе для фильтрации входящих пакетов, и один – для исходящих. Соответственно, все необходимые критерии фильтрации должны быть сформулированы администратором внутри одного списка. В стандартных списках доступа отбор пакетов производится по IP-адресу источника пакета.

Список использованных источников

1. Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс. Андрончик А.Н.
2. Организация защиты сетей Cisco. Уэнстром Майкл.
3. Практика построения компьютерных сетей. Кульгин М.
4. Протоколы TCP/IP. Практическое руководство. Стивенс У. Р.
5. Защита информации в компьютерных сетях. Андрончик А.Н.
6. Cisco Systems. [Электронный ресурс]. Режим доступа: http://www.cisco.com.

АВТОМАТИЗАЦИЯ РАБОТЫ СИСТЕМНОГО АДМИНИСТРАТОРА

Назарити Антон Александрович, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В наше время цифровые технологии занимают наиболее важную часть в современной жизни. Ведь сейчас с помощью компьютеров обеспечиваются многие жизненно важные процессы. Компьютерные технологии делают жизнь человечества удобнее. Люди обладают возможностью в кратчайшие сроки подобрать интересующую их информацию. Электронные вычислительные машины дают людям поистине безграничные возможности. В медицине компьютерное оборудование применяется для проведения диагностических процедур, для лечения пациентов. Практически в любой профессии необходимо использовать программного обеспечение. Ярким случаем зависимости человека от цифровых технологий является автомобиль. Микроконтроллеры, оснащёнными нужными программами и датчиками, управляют почти всеми системами современной машины. Можем наблюдать повсеместное использование компьютерного оборудования в науке, в медицине, в правоохранительных органах и т.д.

Благодаря цифровым технологиям остаётся в прошлом тяжёлый и монотонный человеческий труд, теперь он выполняется автоматическими системами. Они не испытывают голод, жажду и усталость. Поэтому они выполняют монотонную работу лучше, чем люди.

Возрастает потребность в высококлассных специалистах для того, чтобы обслуживать компьютерное оборудование. Появляются новые профессии и специальности. Такой профессией является системный администратор, который осуществляет настройку, ремонт, обслуживание компьютеров и т.д. Без этого специалиста невозможно представить ни одну кампанию или фирму.

В обязанности и задачи системного администратора входят следующие операции:

1) создание резервных копий, их проверка и удаление;
2) установка необходимых обновлений для используемого программного обеспечения;
3) установка и настройка операционных систем;
4) создание пользовательских учетных записей, контроль за их состоянием;
5) обеспечение информационной безопасности;
6) исправление неполадок в оборудовании;
7) создание, расширение сетевой структуры предприятия;
8) Введение документации по выполненным действиям.

Многие из этих операций выполняются ежедневно, они отнимают у специалиста много времени, которое можно потратить на решение более важных задач. В этой ситуации будет полезно применить автоматизацию указанных действий.

Автоматизация выполняемых действий на компьютере важна и актуальна, потому что многократные постоянные операции могут осуществляться без присутствия пользователя. Таким образом, этот процесс сделает работу на ПК более надежной и позволит нам сэкономить немало времени, которое можно потратить на решение других профессиональных задач.

Рассмотрим программы, выполняющие задачи автоматически, в отсутствии пользователя. Одним из таких приложений является встроенная в операционную систему Windows - программа «Планировщик заданий».

Особенность этого приложения заключается в том, что оно осуществляет исполнение заранее запланированных заданий в установленное время, когда появляются определенные события, действия могут выполняться однократно или периодически, через определенные промежутки времени. Задачи также приводят в действие запуск файлов, команд или

программ. Эти задания реализовывают многие операции, обеспечивающие работу системы и сохранение ее в рабочем состоянии.

Планировщик задач поможет нам выполнять такие операции как:

- Дефрагментация диска;
- Удаления с диска ненужных файлов;
- Диагностика системы;
- Создание архиваций в определенное время;

В наше время много ценных данных, важной информации хранится в компьютере. К сожалению, возникают такие ситуации как сбой системы, влияние вредоносных программ, ошибочные действия других пользователей, поломка жесткого диска и так далее… В результате всего этого может произойти утеря файлов, их повреждение, изменение и разрушение. Чтобы не потерять важные документы, данные и сведения необходимо применять резервное копирование.

Резервное копирование (на англ. «backup copy») - это процесс копирования файлов и папок на какой-либо носитель информации с целью их дальнейшего восстановления.

Важным принципом резервного копирования является регулярность. Это значит, что нужно создавать «бэкапы» файлов регулярно. Возьмем в пример ситуацию, когда студент пишет каждый день курсовую работу. Нужно создавать резервную копию этой работы ежедневно, чтобы в случае непредвиденных обстоятельств мы смогли избежать потери результатов труда и все быстро восстановить.

Удобным и надежным решением будет автоматизация этой каждодневной операции.

Мы рассмотрели такую профессию как системный администратор. Проанализировав его задачи и обязанности, мы убедились, что в круг его повседневных действий входит выполнение регулярных операций. Поэтому в системном администрировании применяются процессы автоматизации. Ведь куда удобнее и эффективнее, чтобы повседневные, рутинные задачи выполнялись автоматически, а администратор имел возможность сконцентрировать свое внимание на решении более глобальных проблем.

Список использованных источников

1. Линн.С. Администрирование Microsoft Windows Server 2012 / С. Линн-Питер. -384 С.
2. Кенин А.М. Самоучитель системного администратора / А.М Кенин- БХВ-Петербург. Проект Exiland Backup: [сайт]- URL: https://exiland-backup.com/ru/
3. Планировщик заданий в OCWindows: [сайт]-URL: https://www.comss.ru/page.php?id=4840

ОТЕЧЕСТВЕННАЯ СИСТЕМА LINUX БЕЗОПАСНЕЕ, НАДЁЖНЕЕ И БЫСТРЕЕ, ЧЕМ ЗАРУБЕЖНЫЙ WINDOWS

Наконечный Никита Ярославович курант 1 курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Поскольку Windows является широко применяемой операционной системой, то каждый её пользователь время от времени сталкивался с проблемами безопасности и стабильности системы. Windows изначально была разработана с прицелом на однопользовательские ПК без сетевого подключения и не имела встроенных функций безопасности. В Windows вредоносные программы и вирусы легко получают доступ к системным файлам и могут нанести большой ущерб. Кроме того, максимальное количество вирусов создается именно под Windows (учитывая огромную долю рынка). Стоит отметить, что Linux также не застрахован от атак на систему, но если вы будете следовать самым простым правилам и не давать прав суперпользователя всему, что запускаете, то вы, вероятно, будете в большей безопасности, в сравнении с Windows.

Поскольку Windows является широко применяемой операционной системой, то каждый её пользователь время от времени сталкивался с проблемами безопасности и стабильности системы. Windows изначально была разработана с прицелом на однопользовательские ПК без сетевого подключения и не имела встроенных функций безопасности. В Windows вредоносные программы и вирусы легко получают доступ к системным файлам и могут нанести большой ущерб. Кроме того, максимальное количество вирусов создается именно под Windows (учитывая огромную долю рынка). Стоит отметить, что Linux также не застрахован от атак на систему, но если вы будете следовать самым простым правилам и не давать прав суперпользователя всему, что запускаете, то вы, вероятно, будете в большей безопасности, в сравнении с Windows.

Кроме того, если вы являетесь пользователем Windows, то вам придется выработать привычку перезагружать систему практически после каждого чиха:

Только что установили программу — перезагрузка!

Удалили программу — перезагрузка!

Пришли обновления Windows — перезагрузка!

Система стала медленнее работать — вы правильно догадались, перезагрузка!

Однако в случае с Linux вы можете спокойно продолжать свою работу, и ваша ОС не будет вас беспокоить.

Linux за последние годы достиг значительных результатов в плане улучшения качества и удобства своего применения. Дистрибутивы, такие как Linux Mint и Ubuntu, даже дошли до того, что упростили свою установку и настройку для далеких от техники пользователей, чтобы они могли с максимальной легкостью выполнять повседневную работу.

Windows, из-за её распространения, является стандартной ОС на многих устройствах. Пользователи уже настолько привыкли нажимать на «Пуск» и открывать свои любимые программы, что им очень трудно переключиться на что-то другое.

В Microsoft Windows файлы хранятся в каталогах/папках на разных дисках (диски C:\, D:\, E:\ и т.д.). В то время как в Linux файлы и папки, начиная с корневого каталога, упорядочены в виде древовидной структуры, разветвляясь на различные подкаталоги.

В Linux всё представляется и обрабатывается, как будто вы имеете дело с файлом. Каталоги — это файлы, файлы — это файлы, внешние подключенные устройства (такие как принтер, мышь, клавиатура) — тоже являются файлами.

Linux предлагает большую скорость и безопасность, с другой стороны, Windows предлагает большую простоту использования, так что даже далекие от компьютеров люди могут легко работать с данной ОС.

Linux используется многими корпоративными организациями в качестве серверной ОС, обеспечивая безопасность для всей IT-инфраструктуры, в то время как Windows в основном используется обычными пользователями и геймерами.

На мой взгляд, нет одного лидера. Обе ОС являются уникальными и наилучшим образом соответствуют конкретным требованиям пользователей и потребностям

КЛАССИФИКАЦИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Нечаев Антон Алексеевич, курсант 2-го курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В соответствии с федеральным законом от 27 июля 2006 года **№ 149-ФЗ** (ред. от 29.07.2017 года) «Об информации, информационных технологиях и о защите информации», статья 7, п.1 и п.4:

1. Защита информации представляет собой **принятие правовых, организационных и технических мер**, направленных на:

- **Обеспечение** защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- **Соблюдение** конфиденциальности информации ограниченного доступа;
- **Реализацию** права на доступ к информации.

Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, **обязаны обеспечить**:

- **Предотвращение** несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- Своевременное **обнаружение** фактов несанкционированного доступа к информации;
- **Предупреждение** возможности неблагоприятных последствий нарушения порядка доступа к информации;
- **Недопущение** воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- Возможность незамедлительного **восстановления** информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- Постоянный **контроль** за обеспечением уровня защищенности информации;
- **Нахождение** на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации (п. 7 введен Федеральным законом от 21.07.2014 **№ 242-ФЗ**).

Исходя из закона **№ 149-ФЗ** защиту информации можно разделить так же на несколько уровней:

1. **Правовой уровень** обеспечивает соответствие государственным стандартам в сфере защиты информации и включает авторское право, указы, патенты и должностные инструкции.
2. Грамотно выстроенная система защиты не нарушает права пользователей и нормы обработки данных.
3. **Организационный уровень** позволяет создать регламент работы пользователей с конфиденциальной информацией, подобрать кадры, организовать работу с документацией и носителями данных.
4. Регламент работы пользователей с конфиденциальной информацией называют правилами разграничения доступа. Правила устанавливаются руководством компании совместно со службой безопасности и поставщиком, который внедряет систему безопасности. Цель – создать условия доступа к информационным ресурсам для каждого пользователя, к примеру, право на чтение, редактирование, передачу конфиденциального документа.
5. Правила разграничения доступа разрабатываются на организационном уровне и внедряются на этапе работ с технической составляющей системы.

6. **Технический уровень** условно разделяют на физический, аппаратный, программный и математический (криптографический).

Средства защиты информации принято делить на **нормативные (неформальные)** и **технические (формальные)**.

Неформальными средствами защиты информации – являются нормативные(законодательные), административные(организационные) и **морально-этические** средства, к которым можно отнести: документы, правила, мероприятия.

Правовую основу (**законодательные средства**) информационной безопасности обеспечивает государство. Защита информации регулируется международными конвенциями, Конституцией, федеральными законами «Об информации, информационных технологиях и о защите информации», законы Российской Федерации «О безопасности», «О связи», «О государственной тайне» и различными подзаконными актами.

Так же некоторые из перечисленных законов были приведены и рассмотрены нами выше, в качестве правовых основ информационной безопасности. Не соблюдение данных законов влечет за собой угрозы информационной безопасности, которые могут привести к значительным последствиям, что в свою очередь наказуемо в соответствии с этими законами в плоть до уголовной ответственности.

Государство также определят меру ответственности за нарушение положений законодательства в сфере информационной безопасности. Например, глава 28 «Преступления в сфере компьютерной информации» в Уголовном кодексе Российской Федерации, включает три статьи:
Статья 272 «Неправомерный доступ к компьютерной информации»;

- Статья 273 «Создание, использование и распространение вредоносных компьютерных программ»;
- Статья 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей».

Административные (организационные) мероприятия играют существенную роль в создании надежного механизма защиты информации. Так как возможности несанкционированного использования конфиденциальных сведений в значительной мере обусловливаются не техническими аспектами, а злоумышленными действиями. Например нерадивостью, небрежностью и халатностью пользователей или персонала защиты.

Для снижения влияния этих аспектов необходима совокупность организационно-правовых и организационно-технических мероприятий, которые исключали бы или сводили к минимуму возможность возникновения угроз конфиденциальной информации.

В данной административно-организационной деятельности по защите информационной для сотрудников служб безопасности открывается простор для творчества.

Это и архитектурно-планировочные решения, позволяющие защитить переговорные комнаты и кабинеты руководства от прослушивания, и установление различных уровней доступа к информации.

С точки зрения регламентации деятельности персонала важным станет оформление системы запросов на допуск к интернету, внешней электронной почте, другим ресурсам. Отдельным элементом станет получение электронной цифровой подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам электронной почты.

К морально-этическим средствам можно отнести сложившиеся в обществе или данном коллективе моральные нормы или этические правила, соблюдение которых способствует защите информации, а нарушение их приравнивается к несоблюдению правил поведения в обществе или коллективе. Эти нормы не являются обязательными, как законодательно утвержденные нормы, однако, их несоблюдение ведет к падению авторитета, престижа человека или организации.

Формальные средства защиты информации

Формальные средства защиты – это специальные технические средства и программное обеспечение, которые можно разделить на физические, аппаратные, программные и криптографические.

Физические средства защиты информации – это любые механические, электрические и электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним.

Замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами. Группа дополняется средствами систем безопасности, например, видеокамерами, видеорегистраторами, датчиками, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения технических средств для снятия информации.

Аппаратный средства защиты информации – это любые электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы: специальные компьютеры, системы контроля сотрудников, защиты серверов и корпоративных сетей. Они препятствуют доступу к информации, в том числе с помощью её маскировки.

К аппаратным средствам относятся: генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, «перекрывающих» потенциальные каналы утечки информации или позволяющих их обнаружить.

Программные средства защиты информации – это простые и комплексные программы, предназначенные для решения задач, связанных с обеспечением информационной безопасности.
Примером комплексных решений служат DLP-системы и SIEM-системы.

DLP-системы («Data Leak Prevention» дословно «предотвращение утечки данных») соответственно служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков.

SIEM-системы («Security Information and Event Management», что в переводе означает «Управление событиями и информационной безопасностью») обеспечивают анализ в реальном времени событий (тревог) безопасности, исходящих от сетевых устройств и приложений. SIEM представлено приложениями, приборами или услугами, и используется также для журналирования данных и генерации отчетов в целях совместимости с прочими бизнес-данными.
Программные средства требовательны к мощности аппаратных устройств, и при установке необходимо предусмотреть дополнительные резервы.

Математический (криптографический) – внедрение криптографических и стенографических методов защиты данных для безопасной передачи по корпоративной или глобальной сети.

Криптография считается одним из самых надежных способов защиты данных, ведь она охраняет саму информацию, а не доступ к ней. Криптографически преобразованная информация обладает повышенной степенью защиты.

Внедрение средств криптографической защиты информации предусматривает создание программно-аппаратного комплекса, архитектура и состав которого определяется, исходя из потребностей конкретного заказчика, требований законодательства, поставленных задач и необходимых методов, и алгоритмов шифрования.

Сюда могут входить программные компоненты шифрования (криптопровайдеры), средства организации VPN, средства удостоверения, средства формирования и проверки ключей и электронной цифровой подписи.

Средства шифрования могут поддерживать алгоритмы шифрования ГОСТ и обеспечивать необходимые классы криптозащиты в зависимости от необходимой степени защиты, нормативной базы и требований совместимости с иными, в том числе, внешними системами. При этом средства шифрования обеспечивают защиту всего множества

информационных компонент в том числе файлов, каталогов с файлами, физических и виртуальных носителей информации, целиком серверов и систем хранения данных.

УГРОЗЫ, СВЯЗАННЫЕ С РАЗВИТИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Никитин Глеб Константинович, студент 3-го курса
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В настоящее время происходит интенсивное развитие процессов информатизации, которая затрагивает практически все сферы жизнедеятельности человека и аппарата управления. Данная тенденция приводит к формированию новой информационной инфраструктуры, под действием которой появляются новые общественные отношение, регулирование которых не успевает за ходом внедрения информационно-телекоммуникационных технологий в жизнь.

Информационно-телекоммуникационные технологии на данный момент решает следующие задачи:

Электронный обмен данными;

Электронный бизнес;

Удалённое обслуживание клиентов;

Электронная почта;

Высокоскоростная передача пакетов данных;

Внутризоновая, международная связь;

Средства массовой информации;

Предоставление досуга, видеохостинг.

Согласно статистических данных, представленных Федеральной службой государственной статистки, в 2011–2018 гг. в России наблюдался активный рост числа абонентов широкополосного доступа к интернету (ШПД) в расчете на 100 человек населения. По фиксированному интернету прирост составил 76%, мобильному – 80%. За последние 11 лет число абонентов фиксированного ШПД увеличилось в 6 раз. [1]

По данным Международного союза электросвязи, в 2018 г. в мире на 100 человек населения приходилось 14.1 абонента фиксированного и 69.3 – мобильного интернета. [2]

Согласно данным Международного союза электросвязи, в 2018 г. интернетом пользовался каждый второй житель Земли (51.2%). Аудитория интернет-пользователей в России также ежегодно увеличивается. Более двух третей (69%) россиян в возрасте 15–74 лет пользуются им ежедневно, еще 11% – не реже одного раза в неделю.

Согласно статистическим данным, полученных в ходе опроса граждан, который проводил Национальных исследовательский университет Высшая школа экономики, был получен результат, что готовность населения к дистанционным операциям, связанным с финансовыми услугами, в России составляет 40%. [3]

По данным приведённым в Единой межведомственной информационно-статистической системе, среди российских пользователей интернета доля столкнувшихся с угрозами информационной безопасности 27.9% в 2018 г. Основными проблемами остаются несанкционированная рассылка, или спам (с ним сталкивались 19.7% взрослого населения, выходившего в сеть), а также заражение вирусами, приведшее к потере информации и/или времени на удаление (8.9%). [4]

Развитие информационно-телекоммуникационных технологий изменяет вектор преступности в целом. Преступления «уходят с улиц» и переходят в сферу «анонимности», согласно последним данным, а именной краткой характеристики состояния преступности в Российской Федерации за январь-февраль 2021 года, выпущенной Министерство внутренних дел Российской Федерации 19 марта 2021 года, за два месяца текущего года в Российской Федерации зарегистрировано на 29,4% больше IT-преступлений, чем год назад, в том числе совершенных с использованием сети «Интернет» – на 48,3% и при помощи средств мобильной связи – на 32,6%. Если в январе-феврале 2020 года удельный вес преступлений в IT-сфере составлял 19,3%, то за первые 2 месяца текущего года он увеличился до 26,3%. [5]

Это и обуславливает некоторые общие тенденции развития современным информационно-телекоммуникационных технологий, такую как конвергенция и ликвидация промежуточных сведений от источника информации к её потребителю.

Первая тенденция говорит об исчезновении различия между промышленными изделиями и услугами, информационным продуктом и средствами его получения. Происходит диверсификация видов деятельности предприятий, взаимопроникновение различных отраслей промышленности, финансового и торгового секторов, сферы услуг. Объединение разноуровневых компьютерных сетей, обеспечивающих обработку информации.

Вторая заключается в разработке новых методов преобразования информации в удобные и доступные формы для немедленного использования потребителем, тем самым ликвидирует промежуточные звенья производства и ускоряет получение, передачу или отправку документации, денежных средств и тому подобное.

Для понимания этого, можно посмотреть в приложения своего смартфона и увидеть там приложение мобильного банка, портала государственных услуг Российской Федерации и другие приложения, позволяющие быстро совершить какую-либо операцию, используя лишь один телефон и подключение к сети Интернет.

Однако данное удобство и просто для пользователя приводит и к угрозе его безопасности, которая включает в себя незаконное собирание, распространение персональных данных и мошенничество в сфере компьютерной информации.

Нарушение безопасности происходит совершения компьютерных атак, которые можно разделить на сами компьютерные атаки, они в свою очередь будут включать атаки на информационную инфраструктуру Российской Федерации, атаки с использованием программ-шифровальщиков, атак типа «отказ в обслуживании», и атаки с использованием социальной инженерии.

Для недопущения нарушения безопасности при работе с информационно-телекоммуникационными технологиями предлагаю использовать ряд методических рекомендаций.

По предотвращению компьютерных атак:

использование антивирусного программного обеспечения на компьютерах пользователей и серверах, а также своевременное обновление его баз;

регулярный мониторинг и установка исправлений (патчей) безопасности распространенного офисного программного обеспечения и операционных систем;

регулярное обновление сигнатур для систем IDS/IPS и подписок идентификации и анализа киберугроз (Threat Intelligence) для своевременного детектирования подозрительного трафика и поведения;

своевременный вывод из эксплуатации неподдерживаемого производителем программного обеспечения в случае наличия такой возможности;

проведение политики ограничения использования учетных записей с повышенными привилегиями, ограничение количества учетных записей локальных администраторов;

использование паролей, соответствующих требованиям безопасности;

исключение хранения в открытом виде;

выполнение всех рекомендаций по работе с вложениями, пришедшими из подозрительных источников, в том числе рекомендаций не открывать вложения – исполняемые файлы и не включать макросы в документах Microsoft Office, если нет уверенности в надежности отправителя;

отказ в подтверждении доступа, вызывающих сомнение программ.

По противодействию атакам с применением социальной инженерии:

не переходите по неизвестным ссылкам, не перезванивайте по сомнительным

номерам. Даже если ссылка кажется надежной, а телефон верным, всегда сверяйте адреса с доменными именами официальных сайтов организаций, а номера проверяйте в официальных справочниках;

никому не сообщайте персональные данные, а уж тем более пароли и коды;

не храните данные карт на компьютере или в смартфоне;

не доверяйте всей получаемой информации, проверяйте её;

установите и обязательно обновляйте антивирусные программы на всех используемых устройствах.

Список использованных источников

1. Федеральная служба государственной статистки // Росстат URL:
2. https://rosstat.gov.ru/search?q=информационно+телекоммуникационные+технологии (дата обращения: 28.03.2021).
3. Международный союз электросвязи // МСЭ URL:
4. https://www.itu.int/itu-d/sites/statistics/ (дата обращения: 28.03.2021).
5. Институт статистических исследований и экономики знаний // НИУ ВШЭ URL:
6. https://issek.hse.ru/ (дата обращения: 28.03.2021).
7. Единая межведомственная информационно-статистическая система // ЕМИСС
8. URL: https://rosstat.gov.ru/emiss (дата обращения: 28.03.2021).
9. Краткая характеристика состояния преступности в Российской Федерации за
10. январь-февраль 2021 года // МВД РФ URL: https://мвд.рф/reports/item/23447482/ (дата обращения: 28.03.2021).

РАЗРАБОТКА И МОДЕЛИРОВАНИЕ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ УЧАСТКА ТЕРМООБРАБОТКИ СТАНА 350 СПЦ-2 АО «ОЭМК ИМ. А.А. УГАРОВА

Носикова Валерия Викторовна, студентка 4-го курса
Научный руководитель Азарова Виктория Сергеевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Автоматизация технологических процессов является решающим фактором в повышении производительности труда и улучшении качества выпускаемой продукции.

Современными прокатными станами, как и другим металлургическим оборудованием, должны управлять системы автоматики, способные устанавливать наилучшие режимы работы агрегатов и поддерживать, в необходимых пределах, основные технологические параметры, создающие условия для получения требуемых количеств готовой продукции высокого качества.

Автоматизация технологических процессов значительно повышает культуру производства и значительно облегчает труд человека, позволяет переложить выполнение тяжелой физической работы на плечи автоматики. При внедрении автоматизированных систем, функции рабочего сводятся к контролю за работой машин. Наряду с этим улучшаются ход технологического процесса и качество продукции.

Целью исследования является расширенный анализ автоматизированной системы управления термической печи СПЦ-2 АО «ОЭМК им. А.А. Угарова»

Задачи исследования:

- представить краткую характеристику технологического процесса участка термообработки в потоке стана 350;
- произвести анализ существующего уровня автоматизации системы управления термической печью;
- выявить недостатки существующей системы управления;
- опередить задачи на модернизацию системы.

Объектом исследования является участок термообработки стана 350 СПЦ-2 АО «ОЭМК им. А.А. Угарова»

Предмет исследования автоматизированная система управления термической печи СПЦ-2 АО «ОЭМК им. А.А. Угарова».

Сортопрокатный цех N°2 предназначен для производства проката круглого, квадратного, шестигранного и полосового сечений из подшипниковых, рессорно-пружинных и легированных конструкционных сталей [5].

Участок термообработки в потоке стана является частью сложного технологического процесса при производстве проката мелкого сорта.

Участок включает следующее оборудование: устройства для передачи пакетов прутков или бунтов (бунты на поддонах) в термические печи и из термических печей, транспортные устройства, вязальные машины для обвязки пакетов прутков после термообработки, весы для пакетов, устройства для сбора термообработанных пакетов прутков, транспортные устройства для передачи термообработанных бунтов к крюковому конвейеру, склад поддонов для бунтов.

Для термической обработки пакетов прутков и бунтов с использованием тепла прокатного нагрева предусмотрены три проходные термические печи с шагающими балками.

Печи отжига предназначены для проведения термообработки проката с целью предупреждения образования флаконов, получения необходимой твердости металла в соответствии с требованиями научно технической документации и для обеспечения технологичности при обточке.

Отжиг — вид термической обработки металлов и сплавов, заключающийся в нагреве до определённой температуры, выдержке и последующем медленном охлаждении. При отжиге осуществляются процессы возврата (отдыха металлов), рекристаллизации и гомогенизации [2].

Цели отжига — снижение твёрдости для повышения обрабатываемости, улучшение структуры и достижение большей однородности металла, снятие внутренних напряжений. На производстве особое внимание уделяется режиму отжига, который должен очень точно выдерживаться, так как даже незначительные отклонения температуры нарушают технологический процесс, из-за чего отжигаемый прокат не будет обладать тем качеством, которое отмечено в технологической карте.

Назначение печей отжига термическая обработка пакетов и бунтов в проходном или садочном режимах.

Печи предназначены для термообработки проката по следующим трем режимам:

Режим № 1 - задача металла, имеющего температуру 650-680 ˚С, в печь, нагрев его до 760-780 ˚С, выдержка при этой температуре в течение 1 часа, охлаждение в печи до 700 ˚С в течение 2 часов, далее охлаждение на воздухе;

Режим № 2 - задача металла, имеющего температуру 650-680 ˚С, в печь и выдержка его в печи в течение 2 часов и последующее его охлаждение на воздухе;

Режим № 3 - задача металла, имеющего температуру 760-780 ˚С, в печь, охлаждение металла в печи с этой температуры до 650 ˚С в течение 2-3 часов с последующим охлаждением на воздухе.

Производительность термической печи зависит от времени термообработки и от заполнения пода печи металлом.

Проведенный анализ показал, что в настоящее время АСУ печей отжига СПЦ-2 состоит из следующих основных составных частей (промышленного контроллера Simatic S5-155 U, промышленного контроллера Simatic S5-95 F, системы визуализации Coros LS-B и промышленных регуляторов Sipart DR-24).

Контроллер Simatic S5-155 U предназначен для обработки поступающих от операторского терминала значений, хранения пользовательских программ отжига, передачи обработанных уставок температур для камер сгорания в регуляторы Sipart DR-24.

В контроллере Simatic S5-95 F реализован алгоритм безопасности всей промышленной установки.

Система визуализации Coros LS-B представляет собой операторский терминал для отображения текущего состояния технологического процесса, ввода оператором поста управления уставок по температуре в печном пространстве, уставок по расходу природного газа и воздуха, давления в печном пространстве, а также для хранения архивов, отражающих измеренные величины важных параметров печи.

Промышленные регуляторы Sipart DR-24 предназначены для непосредственного управления контрольно-измерительными приборами и исполнительными механизмами. В них запрограммирован алгоритм управления исполнительными механизмами для поддержания заданной температуры в камерах сгорания [3].

Промышленные регуляторы выполняют функции:

- контроля (рабочих режимов технологических параметров, положения исполнительных органов, состояния исполнительных элементов);
- формирования сигналов управляющих воздействий на исполнительные механизмы;
- формирования на лицевой панели световой сигнализации о режимах работы Sipart DR24;
- представления информации о текущих значениях технологических параметров;
- программной реализации технологических алгоритмов контроля и управления тепловыми процессами в ручном и автоматическом режимах;
- передачи текущих значений контролируемых тепловых параметров печи на рабочую станцию оператора-технолога;

- приема уставок и заданий на режим работы Sipart DR24 от рабочей станции оператора-технолога.

В свою очередь, три промышленных контроллера Simatic S5-155 U связаны с терминалами оператора.

В настоящее время существуют следующие контуры автоматического контроля и регулирования:

- температуры в зонах нагрева 1 – 12;
- температуры после вентиляторов рециркуляции № 1 – 4;
- общего давления газа и воздуха на печь;
- давления газа и воздуха на боковые горелки (25 – 36);
- давления в печи;
- общего расхода воздуха на печь;
- общего расхода газа на печь.

Термическая обработка пакетов и бунтов в печах отжига – технологическая операция, непосредственно определяющая качество проката. Изменение температуры рабочего пространства печи осуществляется изменением количества газа и воздуха подаваемых в камеры сгорания. Процесс нагрева металла в печи должен проходить с высокой точностью при задании температуры и необходимого соотношения газо-воздушной смеси, подаваемой на горелки печи, а также обеспечивать безопасность ведения технологического процесса. Несоблюдение теплового режима и топливного соотношения «газ - воздух» приводит к возрастанию бракованной продукции и увеличению окалины [4].

В настоящее время регулирование подачи газа и воздуха в каждую зону нагрева осуществляется в зависимости от значений температуры зоны и величины давления газа и воздуха соответственно, с учётом коэффициента соотношения газо–воздушной смеси для всей печи.

Как показал опыт эксплуатации печей поточной термической обработки СПЦ-2, существующая АСУ ТП термических печей имеет несколько следующих недостатков:

- Трудность ведения технологического процесса, обусловленная тем, что в настоящее время расход газа и воздуха не определяется прямыми измерениями, а рассчитывается теоретически по углу открытия заслонок и давлению в газопроводах (воздухопроводах), что вносит большую погрешность в значения расхода топлива, соотношение газо-воздушной смеси и температуры рабочего пространства печи. Вследствие чего - несоответствие теплового режима работы печи и нерациональное использование природного газа.

- Управление отжигом осуществляется посредством задания уставок температур для 12-ти камер сгорания, расположенных на значительном расстоянии от рабочего пространства печи, что обуславливает большую инерционность температур рабочего пространства печи. При этом разница между температурой в камере сгорания и рабочим пространством печи может составлять от 70°С до 250°С. Большая инерционность температур рабочего пространства печи приводит к тому, что задание уставок температур камер сгорания для управления отжигом является очень трудоемким и, требующим постоянной коррекции и внимания оператора, процессом.

- На печах отжига процесс нагнетания воздуха горения осуществляется тремя вентиляторами. Для нормальной работы трех печей в большинстве случаев достаточно одного вентилятора. Однако при процессах продувки и некоторых режимах отжига, работы одного вентилятора бывает недостаточно. Поэтому управление процессом продувки осуществляется вручную. Операторам приходится включать еще один или два вентилятора (включение производится с местного пульта управления, находящегося на отдельной панели). При этом возникает кратковременный неустойчивый процесс работы одного или нескольких вентиляторов, протекающий по синусоидальной кривой, который может привести к выходу из строя соответствующее оборудование. Кроме того, при резком изменении давления регулятор «Общий газ – воздух», управляющий клапаном общего воздуха для печи и реализованный на основе многофункционального устройства Sipart DR 24

фирмы Siemens, не в состоянии оперативно реагировать на быстрое изменение значений давления воздуха из-за инерционности механизмов. В результате этого зачастую гаснут отдельные горелки на печах, загруженных металлом, а значит, происходит нарушение температурного режима отжига металла, увеличивается риск возникновения аварийной ситуации.

- Контроллер Simatic S5-155 U используемый в АСУ в настоящее время снят с производства, в следствии этого существует нехватка запасных частей, а именно аналоговых модулей ввода/вывода, дискретных модулей ввода/вывода, модулей связи и т.п. Программное обеспечение используемое контроллером морально устарело и является на сегодняшний день достаточно неудобным в использовании и требует высоко квалифицированного персонала [2].

Всё это говорит о целесообразности модернизации автоматизированной системы управления печей отжига на участке термической обработки проката. Решение этой проблемы является основной задачей данного исследования.

Для устранения выявленных недостатков необходимо, чтобы автоматизированная система управления печами отжига обеспечивала рациональное использование энергоресурсов, поддержание высокопроизводительной работы технологического оборудования, оптимизацию технологических параметров нагрева, безопасность технологического процесса.

Задачи модернизации:

- Разработать систему автоматизации печей отжига на управление соотношением газо-воздушной смеси через задание уставок в каждой тепловой зоне печи. Для прямого измерения расхода газа и воздуха требуется установить расходомеры в питающие магистрали.

- Разработать систему автоматизации АСУ ТП печей отжига на управление температурой в камерах сгорания через задание уставок тепловых зонах рабочего пространства печи.

- Привести изображения на станции визуализации в соответствие с новыми алгоритмами управления технологическим процессом и учесть новые параметры для отображения на графиках и сохранения их в архивах измеренных значений для возможности последующего анализа.

- В подсистеме управления и регулирования следует заменить морально устаревший контроллер Simatic 5-го поколения на более совершенный 7-го.

В программе для контроллера S7 необходимо учесть дополнительные контуры регулирования:

- Регулирование соотношения газ-воздух на горелках.

- Регулирование расхода газа.

- Регулирование расхода воздуха.

- Регулирование температуры в камерах сгорания через задание уставок в тепловых зонах рабочего пространства печи.

В системе визуализации необходима корректировка программного обеспечения для отображения и контроля дополнительных контуров регулирования.

Модернизация управления температурного режима печи отжига СПЦ-2 позволит снизить расход топлива и повысить качество производимого металла, за счет точного соблюдения температурного режима отжига, автоматически регулировать ход технологического процесса, уменьшить выбросы в атмосферу вредных веществ.

Список использованных источников

1. Иванов, А. А. Автоматизация технологических процессов и производств. Учебное пособие / А.А. Иванов. - М.: Форум, Инфра-М, 2015. - 224 с

2. Клюев А.С., Лебедев А.Т. Наладка средств автоматизации и автоматических систем регулирования. Справочное пособие - М.: Энергоатомиздат, 2016 - 368с.

3. Котов К.И. Шершевер М.А. Средства измерения, контроля и автоматизации технологических процессов. Вычислительная и микропроцессорная техника. / К.И. Котов, М.А Шершевер. - М.: Металлургия, 2016. - 213 с.

4. Щагин А.В. Основы автоматизации технологических процессов: Учебное пособие для СПО / А.В. Щагин, В.И. Демкин, В.Ю. Кононов, А. Кабанова. - Люберцы: Юрайт, 2016. - 57 с.

5. Оскольский электрометалургический комбинат [Электронный ресурс] www.metalloinvest.com

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ BIG DATA В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Осипова Александра Анатольевна, заместитель командира взвода 3-го курса,
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Проживая в новой эпохе, всё больше и больше задумываешься о том, как развивается мир, какие технологии внедряются в нашу жизнь и как они влияют на будущее. Общий объем обращаемых в Интернете и иных сетях данных подсчитать очень сложно, но мы можем привести некоторые оценочные сведения: по исследованию IDC (International Data Corporation) в 2006 г. весь объем цифровых данных составлял 0,18 зеттабайт, к 2011 г. он должен был увеличиться до 1,8 зеттабайт, в 2018 г. этот показатель составил 33 зеттабайта [1, с. 399], а к 2025 году это будут уже 175 зеттабайт [2, с. 77]; фондовая биржа в Нью-Йорке (https://www.nyse.com) в день генерирует порядка терабайта информации; в проекте Internet Archive хранится более 2 петабайт данных (https://archive.org); эксперименты на Большом адронном коллайдере могут формировать около петабайта данных в секунду [3, с. 143].

В последние годы в сфере аналитики всё чаще употребляется термин «Big Data». Да и не только в аналитике, также и в медицине, финансах, интернет-компаниях и других отраслях. Наше государство на ряду с другими, в последнее время проявляет серьезный интерес к указанным технологиям. В рамках данной статьи нами будет рассмотрено, что представляют из себя «большие данные», области их применения, а также возможности использования в деятельности органов внутренних дел.

Какого-то однозначного подхода к терминологии понятия Big Data («Большие данные») нет, имеются разнообразные мнения на этот счет: согласно докладу Генерального секретаря ООН – это «…накопление и анализ значительно возросшего объема информационных ресурсов, который превышает возможности их хранения и анализа с использованием созданных ранее аппаратных и программных средств» [4, с. 10]; В. С. Овчинский и Е. С. Ларина приходят к выводу, что «…это в первую очередь сырье для различного рода поведенческих технологий, ориентированных на группы достаточно большой размерности, таких как покупатели тех или иных товаров, избиратели, поклонники того или иного бренда, лица, ориентированные на те или иные банковские продукты и т. п.» [5, с. 65]; в другом источнике В. С. Овчинский предлагает другое по своему содержанию определение «…сбор, хранение, оцифровка и предоставление в удобном для пользователя виде в любой точке всей совокупности сведений о тех или иных событиях, процессах, явлениях и т.п.» [6, с. 21]; П. Д. Иванов и В. Ж. Вампилова формулируют следующее понятие «…серия подходов, инструментов и методов обработки структурированных и неструктурированных данных огромных объемов и значительного разнообразия» [7]; достаточно интересным и ёмким является определение сформулированное Oracle Corporation (https://ru.bmstu.wiki/Oracle_Corporation): «…разнообразные данные, которые поступают с постоянно растущей скоростью и объем которых постоянно растет… Три основных свойства больших данных – разнообразие, высокая скорость поступления и большой объем»[1].

Мы же постараемся сформулировать собственное видение данного термина, однако применительно к рассматриваемой в работе тематике. Под «Большими данными» понимается объемное количество разрозненных данных, которые по заданным пользователем характеристикам могут быть обработаны, систематизированы и получен искомый результат. В пример можно привести любую информацию из интернета (в соцсетях, интернет-магазинах, где используется программы лояльностей, фото- и

[1] Сайт «Oracle Россия и СНГ». Режим доступа: URL: https://www.oracle.com/ru/big-data/what-is-big-data.html#close (дата обращения: 05.12.2020).

видеохостингах и т. п.), от разнообразных считывающих устройств, объектов здравоохранения, корпоративной информации и иного.

Каждый шаг, который человек делает в интернете, это «электронный след», то есть данные, фиксируемые в цифровом формате и хранящиеся на различных носителях цифровой информации. Эти данные настолько огромны, что традиционное программное обеспечение для их обработки не может их обработать. Big Data основывается на трёх основных характеристиках:

1. Volume (объем) – это количество информации. Большие данные обрабатываются в очень больших объемах. Они являются неструктурированными или могут быть неизвестного происхождения, могут занимать от нескольких десяток терабайт до сотен петабайт.
2. Variety (разнообразие) – большие данные относятся к многочисленным типам данных. Традиционные типы данных были структурированы и аккуратно вписаны в реляционную базу данных. Однако, с ростом поступающей информации их всё больше относят к неструктурированной, так как они зачастую нечетко сформулированы или требуют дополнительной предварительной обработки (например, аудио, видео или текст).
3. Velocity (скорость) – это скорость, с которой данные принимаются и обрабатываются. Их необходимо обрабатывать так, чтобы какие-то решения на основе этих данных принимались почти в реальном времени. То есть, с точки зрения человека, недолго, иногда долю секунды (например, в поиске), иногда несколько секунд (например, пока пользователь осматривается по сайту) на то, чтобы система подумала, что надо сформировать.

Также к характеристикам больших данных относят: value (ценность), veracity (достоверность) и variability (изменчивость).

Данную технологию следует назвать универсальной, поскольку её использование пригодится в любой сфере деятельности, таких как:

1) предиктивная аналитика или диагностическое обслуживание (использующаяся для поиска потенциального преступника или для мониторинга состояния оборудования с целью выявления и предотвращения сбоев);
2) оптимизация продаж (разработка, снижение стоимости и оптимизация продукции);
3) банковская деятельность (оценка платежеспособностей, улучшение клиентского сервиса);
4) машинное обучение (обучение нейронных сетей);
5) стимулирование инноваций (с помощью изучения взаимозависимости, определения новых способов использования знаний) и многое др.

Благодаря этим обширным способностям больших данных, их возможно применять и в деятельности органов внутренних дел. Одной из главных проблем является установление личности преступников до того, как они начнут противоправные действия и/или после. К примеру, используя информацию, полученную из больших данных потенциально возможно предотвращать тяжкие и особо тяжкие преступления или значительно снизить процент преступности. Однако, то как использовать большие данные в деятельности правоохранительных органов является насущной проблемой, не имеющей простых, тривиальных или готовых решений. Обозначим сферы деятельности ОВД, где они эффективно было бы применение больших данных:

- оперативно-розыскная деятельность;
- административно-правовая деятельность;
- предварительное следствие и дознание;
- экспертно-криминалистическая деятельность;
- деятельность по обеспечению информационной безопасности.

Объем информации, который получает сотрудник ОВД в ходе выполнения своих должностных обязанностей, постоянен и возрастает геометрически без фильтрации и в виде

сплошного потока. Ведь найти преступника среди других миллионов людей это так же, как и найти иглу в стоге сена: установка личности с помощью отпечатков; показаний очевидцев и свидетелей; записей камер видеонаблюдения; установка транспортного средства, использованного при совершении деяния; установка соучастников или других подозреваемых, которые могут быть причастны по системе взаимосвязей; выявление местоположения или маршруты передвижений в определенные периоды времени. На любую необходимую информацию для расследования и раскрытия преступлений или правонарушения нужно время. Например, если это прослушивание телефонных переговоров или просмотр камер видеонаблюдения, то информация обо всех разговорах и действиях фигуранта за значительный промежуток времени. Или это может быть получение данных о движении денежных средств по счетам или по действиям в интернете, то это большой объем информации обо всех операциях за определенный период времени, а сами периоды могут быть продолжительные от нескольких дней до месяцев или лет. Если речь идет о получении компьютерной информации или о получении информации из технических каналов связи, то это работа с обширной информацией из этого источника.

Вся перечисленная неотфильтрованная (несистематизированная, неупорядоченная и т. п.) информация и относится к Big Data, которые позволят правильно поставить конкретные вопросы, установить определенные критерии отбора, использовать специализированное программное обеспечение, то анализ, распознание и получение искомой информации получится быстрый, эффективный, а процесс раскрытия и расследования преступления или правонарушения сократится в разы. А по завершении расследований эти данные следует рассортировать по показателям, совершенствуя разработку и выстраивая «дерево решений», где у каждой ветви имеется свой определенный вес (или же использовать Machine Learning, то есть машинное обучение для более оперативной работы с имеющейся информацией). Тогда при работе над последующими преступлениями сотрудник из задаваемых критериев отбора при помощи подобной технологии смог в кратчайшие сроки находить искомое.

Всё же, несмотря на все положительные моменты внедрения технологии больших данных в правоохранительные органы, есть и обратная сторона:

1. Действующие сотрудники не смогут воспользоваться данной технологией без дополнительного обучения, а лучше всего – это привлечение профильных специалистов, которые разбираются в технологии и смогут эффективно ее эксплуатировать. Указанный недостаток решим, сейчас в системе МВД России есть четыре учебных заведения, подготавливающих технических специалистов: Московский, Санкт-Петербургский и Краснодарский университеты, Воронежский институт.
2. Использование рассматриваемой технологии невозможно без соответствующего программного и технического оборудования. Ведь вся информация больших данных очень объемна, и её надо где-то хранить, обрабатывать, анализировать и т. п.
3. Большие объемы затрат на внедрение технологии. Согласно прогноза уже упоминаемой нами ранее аналитической компании IDC в 2016 г. (более свежих данных найти не удалось) объем мирового рынка программного обеспечения, оборудования и сервисов в бизнес-аналитики и работы с Big Data составил 130,1 млрд долларов. Большая часть расходов пришлась на банковский сектор (13,1% или 17 млрд долларов), дискретное (11,9%), непрерывное производство (8,4%), а также денежные вливания от государственных органов составили 7,6%[2].

[2] Статья «Большие данные (Big Data) мировой рынок». Сайт TAdviser (Государство. Бизнес. ИТ). Режим доступа URL: https://www.tadviser.ru/index.phpСтатья:Большие_данные_(Big_Data)_мировой_рынок#IDC:_.D0.9E.D0.B1.D1.8A.D0.B5.D0.BC_.D1.80.D1.8B.D0.BD.D0.BA.D0.B0_.D0.B2_.24130_.D0.BC.D0.BB.D1.80.D0.B4 (режим доступа: 07.12.2020).

4. Не точность получаемой при анализе больших данных информации. Даже совершенствуя такую технологию для определения (предсказания) возможных правонарушений или потенциальных преступников, алгоритмы будут не всегда выдавать точный ответ, а на полученную информацию (которая может являться не достоверной) сотрудники будут отвлекаться, проверяя ее аутентичность.

5. Коррупционная и/или иная преступная составляющая, которая может повлиять на результат анализа.

6. Сложность интеграцией технологии Big Data в уже существующие и применяемые в ОВД программно-технические решения.

На сегодняшний день на рынке больших данных существуют не малое количество программных решений (с точки зрения конечного пользователя): Apache Spark (Hadoop, Storm, Cassandra) (США), Lumify (США), Elastic (США), Oracle Data Mining (США), Mail.Ru Cloud Solutions (Россия) и иные.

Нельзя сказать, что из-за такого количества недостатков нельзя пользоваться технологией Big Data в деятельности ОВД. Однако в данный промежуток времени, как нам кажется, это не совсем представляется возможным из-за указанных минусов. В свою же очередь, положительные моменты применения подобной технологии очень заманчивы: это и автоматизация анализа большого объема информации, и прогнозирование тех или иных ситуаций (действий, поступков), и оперативная классификация сведений и др. Предположим, что данный перспективный ресурс в дальнейшем будет полноценно внедрен в работу правоохранительных органов, что позволит снизить количество преступлений и успешно раскрывать уже совершенные на территории нашей страны.

Список использованных источников:

1. Кляус О. А., Кляус П. Т. Применение технологий Big Data в современных условиях // Стратегия устойчивого развития в антикризисном управлении экономическими системами. Материалы VI Международной научно-практической конференции. – Донецк, 2020. – С. 395-406.

2. Дейтел П., Дейлел Х. Python: Искусственный интеллект, большие данные и облачные вычисления. – СПб.: Питер, 2020. – 864 с.: ил. – (Серия «Для профессионалов»).

3. Клеменков П. А., Кузнецов С. Д. Большие данные: современные подходы к хранению и обработке // Труды Института системного программирования РАН. – Ч. 23. – 2012. – С. 143-158.

4. Доклад Генерального секретаря ООН «Использование информационно-коммуникационных технологий для инклюзивного социально-экономического развития. Семнадцатая сессия. – Женева, 12-16 мая 2014 года. – 26 с.

5. Искусственный интеллект. Большие данные. Преступность / В. С. Овчинский, Е. С. Ларина. – «Книжный мир», 2018. – 188 с. – (Коллекция Изборского клуба).

6. Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. – М. : Норма : ИНФРА-М, 2018. – 352 с.

7. Иванов П. Д., Вампилова В. Ж. Технологии Big Data и их применение на современном промышленном предприятии // Инженерный журнал: наука и инновации. – № 8 (32). – 2014 [электронный ресурс].

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ СТЕНДА СУШКИ И ПРЕДВАРИТЕЛЬНОГО РАЗОГРЕВА ВАКУУМ-КАМЕРЫ ЭСПЦ АО «ОЭМК ИМ. А.А.УГАРОВА»

Палагин Виктор Владимирович, студент 4-го курса
Научный руководитель Горюнова Марина Владимировна, преподаватель высшей категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО «Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Электросталеплавильный цех является одним из основных цехов АО «ОЭМК им. А.А.Угарова». В нём в процессе внепечной обработки стали используются установки для циркуляционного вакуумирования стали.

Установки предназначены для удаления растворенных в жидкой стали газов (водорода, азота, оксида углерода) и посторонних элементов (серы, фосфора). При вакуумировании также происходит продувка металла инертными газами, добавление легирующих элементов для придания стали определенных физических, химических, механических или эксплуатационных свойств [4].

Технология процесса циркуляционного вакуумирования заключается во всасывании жидкой стали из сталеразливочного ковша и циркуляции его в вакуум-камере через входной и выходной патрубок и дегазации в ней стали, в ковш погружается выложенный огнеупором всасывающий патрубок, который крепится на вакуум-камере, футерованной огнеупорным материалом.

Перед использованием вакуум- камеры, её необходимо нагреть до высокой температуры, чтобы предотвратить повреждение дорогостоящей футеровки при контакте с расплавленной сталью.

Целью исследования является анализ автоматизированной системы управления стенда сушки и предварительного разогрева вакуум-камеры ЭСПЦ АО «ОЭМК им. А.А.Угарова».

Задачи исследования:

- изучить характеристику технологического процесса и технологические параметры стенда сушки и предварительного разогрева вакуум-камеры;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является стенд сушки и предварительного разогрева вакуум-камеры ЭСПЦ АО «ОЭМК им. А.А.Угарова».

Предметом исследования является автоматизированная система управления стенда сушки и предварительного разогрева вакуум-камеры ЭСПЦ АО «ОЭМК им. А.А.Угарова».

Объектом автоматизации является стенд сушки и предварительного разогрева вакуум-камеры (ССРВК) на УПА №1, установленного в электросталеплавильном цехе АО «ОЭМК им. А.А.Угарова». Стенд предназначен для сушки и предварительного разогрева футеровки вакуум-камеры после её ремонта в футеровочном отделении и перед установкой на УЦВС.

Стенд состоит из газокислородной горелки с трубопроводами, водоохлаждаемой крышки, механизма подъема-опускания крышки, контрольно-измерительных приборов.

Техническая характеристика газокислородной горелки:

Тип: ГСВ-01, количество на стенде -1 шт.

Топливо: природный газ

- состав природного газа: CH_4; C_2H_6; C_3H_8; C_4H_{10}; C_5H_{12}; CO_2; N_2; O_2 ;
- давление газа в газопроводе 0,3 МПа;
- номинальное (рабочее) давление газа 0,28 МПа;

Кислород на горение:

- давление кислорода в кислородопроводе 1,2 МПа;

- давление перед горелкой после редуктора (КРД-1) 0,6 МПа.

Тепловой режим стенда:

- температура нагрева до 1200 °С.

Расход природного газа:

- максимальный 70 $м^3$/ч;
- номинальный (рабочий) 66 $м^3$/ч;
- минимальный 20 $м^3$/ч.

Расход кислорода:

- максимальный 143 $м^3$/ч;
- номинальный (рабочий) 140 $м^3$/ч;
- минимальный 42 $м^3$/ч.

Существующая АСУ ТП УПА №1 выполняет следующие функции:

- контроля и управления процессом продувки стали;
- решения задач, связанных с контролем состояния оборудования, сбором, хранением и первичной обработкой информации;
- сетевой передачи информации о расходах энергоносителей в вышестоящие цеховые и коммерческие автоматизированные системы для формирования отчетных и сопроводительных документов.

На АСУ ТП УПА №1 возможен дистанционный (ручной) режим управления, т. е. сталевар и подручный сталевара с пульта при помощи кнопок могут осуществлять управление механизмами и агрегатами установки. АСУ ТП УПА № 1 осуществляет регистрацию расходов аргона; регистрацию аварийных, рабочих и др. сообщений, архивирование данных процесса в виде графиков и таблиц.

Для выполнения указанных функций используется двухуровневая система автоматизации. На первом уровне используют промышленный контроллер “Simatic S7-400” фирмы Siemens, а на втором уровне - операторские станции на базе промышленных персональных компьютеров.

Сталевар и подручный сталевара для выполнения контролирующих и управляющих функций используют операторские станции. Для бесперебойной и удобной работы установлены две операторские станции.

Программное обеспечение станций операторов пульта управления разработано на базе операционной системы WINDOWS-XP и SCADA-системы iFIX.

Основные функции АСУ ТП ССРВК могут быть сгруппированы следующим образом: информационные и информационно-вычислительные функции.

Контроль величин параметров:

- положение клапанов природного газа и кислорода;
- давление на клапанах природного газа и кислорода;
- расход природного газа;
- расход кислорода;
- температура охлаждающей воды водоохлаждаемой крышки на входе;
- температура охлаждающей воды водоохлаждаемой крышки на выходе;
- расход охлаждающей воды на входе;
- расход охлаждающей воды на выходе.

Расчётные функции:

- расчёт технико-экономических показателей.

Управляющие функции.

Управление величинами параметров:

- расходом природного газа;
- расходом кислорода;
- расход технической воды для охлаждения крышки.

Управление процессами:

- розжиг горелки;

- отключение горелки;
- разогрев вакуум-камеры по строго заданной технологической карте.

Кроме приведенного перечня функций, АСУ ТП осуществляет:
- сбор данных с датчиков;
- визуализацию технологического процесса;
- сигнализацию отклонений от норм основных технологических величин;
- регистрацию и сигнализацию аварийных ситуаций;
- архивирование параметров;
- накопление информации о режимах разогрева вакуум-камеры (для последующего анализа);
- генерирование отчетов [1].

Существующая система автоматизации предназначена для управления технологическим процессом, контроля технологических параметров, архивирования значений контролируемых параметров и оперативного их представления технологическому персоналу на экраны цветных операторских станций.

Система построена по иерархическому принципу, имеет 3 уровня: нижний, средний и верхний уровень.

Нижний уровень состоит из датчиков и исполнительных механизмов: исполнительный механизм регулирования расхода природного газа, исполнительный механизм регулирования расхода кислорода, датчик расхода природного газа, датчик расхода кислорода, датчики расходов воды водоохлаждаемой крышки на входе и на выходе, датчики температуры водоохлаждаемой крышки на входе и на выходе, датчик температуры футеровки вакуум-камеры.

Средний уровень состоит из программируемого логического контроллера: “Simatic S7-400” фирмы Siemens.

Верхний уровень состоит из двух автоматизированных рабочих мест: АРМ-1 ROBO-2000-4385TL и АРМ-2 ROBO-2000-4385TL.

До внедрения автоматизированной системы управления режимом работы стенда сушки и предварительного разогрева вакуум-камеры, объект имеет некоторый начальный уровень автоматизации. Объект оснащён средствами дистанционного управления и контроля над процессом. Для определения расхода газа и кислорода используются расходомеры. Полученное от расходомера значение преобразуется в электрический сигнал, который отображается на операторской станции [2].

Для регулирования расхода природного газа и кислорода используются исполнительные механизмы, оснащённые электроприводом, которые дистанционно управляются с помощью кнопок, расположенных на рабочем месте сталевара. С помощью кнопок можно подавать 2 команды: «Закрыть (уменьшить расход)» и «Открыть (увеличить расход)».

Недостатками системы автоматизации стенда сушки и разогрева вакуум-камеры являются:
- затратное использование газокислородной горелки в сравнении с газовоздушной;
- датчики, исполнительные устройства морально и физически устарели, не удовлетворяют современным требованиям, их своевременное обслуживание и ремонт затруднены;
- ручное управление соотношением природный газ/кислород не обеспечивает экономичное и безопасное управление процессом разогрева;
- управление разогревом камеры по технологической карте выполняет сталевар, изменяя вручную расходы газа и кислорода, что не позволяет поддерживать наиболее эффективный режим разогрева;
- отсутствует автоматическая противоаварийная защита: контроль наличия пламени горелки происходит визуально сталеваром через промежутки времени (в паузах между обработкой стали на УПА №1);

- отсутствует сигнализация о погасании факела горелки, не сообщается об отклонении давления природного газа и кислорода от нормы.

В настоящее время система управления стендом сушки и разогрева вакуум-камеры автоматизирована частично, что в свою очередь не обеспечивает необходимого, оптимального регулирования технологических параметров и безопасного его ведения. Целью исследования является автоматизация системы управления процессом сушки и разогрева вакуум-камеры с использованием современных средств измерения, регулирования и безопасности ведения процесса сушки и разогрева.

Автоматическое регулирование, т. е. регулирование с помощью соответствующих приборов, которые, выравнивая и стабилизируя процесс, реагируют на изменения быстрее оператора, является более эффективной формой управления установкой. Перевод стенда сушки и разогрева вакуум-камеры на автоматическое регулирование обеспечит поддержание процесса сушки и разогрева в максимальном приближении к заданным технологической инструкцией кривым разогрева вакуум-камеры, повышение стойкости футеровки, снижение затрат на энергоресурсы и футеровочный материал, ведение процесса будет более безопасно.

Основными целями модернизации существующей системы является:

- обеспечение безопасного технологического режима;
- повышения качества и быстродействия регулирования, и как следствие, достижение высокого уровня стабилизации технологических режимов;
- увеличение срока службы футеровки вакуум-камеры, за счет более точного поддержания заданной температуры вакуум-камеры во время её разогрева и сушки (соблюдение кривых разогрева);
- оптимальное регулирование технологических параметров процесса;
- снижение расхода газа, кислорода, воды и футеровочного материала;
- улучшение условий труда персонала и повышения эффективности их труда за счёт увеличения их безопасности.

Модернизация системы управления стенда сушки и предварительного разогрева вакуум-камеры ЭСПЦ АО «ОЭМК им. А.А.Угарова», заключается в сокращении расхода материалов и энергии, повышении производительности труда путем снижения трудоемкости обслуживания агрегатов и возрастания их производительности, за счет замены морально устаревшего оборудования на актуальное.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. — 2-е изд. — Саратов : Ай Пи Эр Медиа, 2019. — 459 c. — ISBN 978-5-4486-0574-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83341.html. — Режим доступа: для авторизир. пользователей

РАЦИОНАЛИЗАЦИЯ ИСПОЛЬЗОВАНИЯ ОБОРУДОВАНИЯ ПРИ ВАКУУМИРОВАНИИ СТАЛИ

Парамонов Дмитрий Сергеевич, студент 3 курса
Научный руководитель Долгих Антон Александрович, преподаватель,
Гришина Светлана Сергеевна, преподаватель высшей, категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Как известно, одним из главнейших показателей успешного и эффективного производства является экономическая составляющая, а именно, эффективное использование имеющихся на данном производстве технических средств. Зачастую нерациональное использование имеющегося оборудования и материалов негативно отражается на экономических показателях.

Рациональное использование производственных мощностей отражается на финансовых результатах работы предприятия за счет: увеличения выпуска продукции, снижения себестоимости, улучшения качества продукции и увеличения балансовой прибыли.

В сталеплавильном производстве, наряду с процессом выплавки стали, также наиболее энергоёмким процессом является процесс обработки стали в стальковше. Этот процесс называется внепечная обработка, которая может включать в себя обработку металла на агрегате комплексной обработке стали (АКОС), обработку на установке продувки металла инертным газом и процесс вакуумирования жидкой стали.

При обработке металла вакуумом происходит колоссальные затраты электроэнергии на создание вакуума. Вакуум получают за счёт пароэжекторных насосов, для работы которых необходимо большое количество перегретого пара. Параметры работы пароэжекторного насоса и кинетики протекания реакций обезуглероживания в процессе внепечной обработки представлены в работе [2].

Вакуумная обработка металла может производится по двум режимам работы пароэжекторного насоса: экономичный режим и режим с повышенной нагрузкой. В зависимости от цели вакуумирования и сортамента стали разряжение в вакуум-камере может меняться в широком интервале – от 0,5 до 70 мм рт. ст.[1].

Кроме работы пароэжекторных насосов, в статью затрат можно отнести расход футеровочных материалов, заправочной массы для подварки патрубков ваккууматора, время на ремонт и восстановления футеровки вакуум-камеры, время на демонтаж отработанной вакуум-камеры и монтаж новой камеры, трудозатраты на текущее обслуживание установки и др.

Для того, чтобы снизить затраты целесообразно будет рационализировать процесс работы оборудования в процессе вакуумирования стали. Так как основной целью этого процесса является дегазация стали, то и оперироваться необходимо в основном на этот показатель, взяв во внимание остаточное содержание водорода, которое выражается в парциальном давлении (ppm) и зависит, в основном, от разряжения в вакуум-камере и от времени вакуумирования.

Понижение давления над жидким металлом может вызвать удаление растворенных в нем газов (водорода и азота). Кроме растворенных газов, в атмосферу могут удаляться в газообразном состоянии и металлические примеси, упругость паров которых выше давления в системе. Поэтому на разное состояние при нормальных условиях и разные формы существования в стальном расплаве газов и металлических примесей, существуют общие закономерности их удаления из расплава при вакуумной плавке или обработке стали.

Удаление газов при вакуумировании стали обусловлено уменьшением их парциального давления в атмосфере при уменьшении общего давления над сталью в результате вакуумирования [3].

Водород и азот содержатся в стали в количествах, обычно превышающих равновесные и при парциальных давлениях, достигаемых в вакуумных агрегатах, поэтому при вакуумировании имеются термодинамические предпосылки для их удаления. Однако процессы удаления в вакууме газов (водорода и азота) и металлических примесей вследствие непрерывной откачки выделяющихся газов и конденсации паров на сравнительно холодных частях установок носят ярко выраженный неравновесный характер, поэтому оценку этих процессов более правильно проводить не с точки зрения термодинамического равновесия, а с точки зрения кинетики удаления.

Основываясь на опытных данных можно вывести зависимость содержания H_2от времени вакуумирования при постоянном значении разряжения, равном 0,8-1,1mbar.

Рисунок 1 – График зависимости содержания водорода в стали от времени вакуумирования

Из графика (рис.1) видно, что основная часть H_2 (80-85%) уходит из стали за первые 12-15 минут вакуумирования, что соответствует содержанию 1,3-1,45ppm. При дальнейшей работе вакуум-камеры удаление водорода происходит незначительно.

Большинство современных предприятий, в том числе и ОЭМК, не ограничивается производством конкретных марок стали, а имеет в своей разработке различное множество марок стали. Марки стали, производимые на предприятии имеют различный химический состав, и соответственно, различную схему и способ обработки. Кроме этого, по требованию заказчиков, стали имеют разные заданные пределы по содержанию водорода. Учитывая эти требования, время обработки металла вакуумом можно производить в зависимости от заданных пределов для конкретной марки стали, рационализируя ресурс используемого оборудования.

Марки стали по содержанию водорода разделяют на различные группы, с разным содержанием водорода (не более 2 ppm, не более 2,5 ppm, не более 3 ppm, не более 4 ppm и с H_2 не более 5 ppm). Таким образом, марочник с регламентированным содержанием водорода необходимо обрабатывать вакуумом, с различным временем исходя из графика (рис.1).

На основании практических данных, марки стали можно сделать вывод что, стали целесообразно обрабатывать вакуумом при содержании водорода не более 2 ppm - 15-20 мин., при H_2 от 2,5 до 3 ppm – 15-18 мин., при H_2 более 3ppm – 10-12 мин. (табл.1).

Таблица 1 – Время обработки в вакуум-камере, в зависимости от содержания водорода в марке стали.

Содержание водорода, не более	2 ppm	2,5 ppm	3 ppm	4 ppm	5 ppm

Время вакуумирования, мин	15-20	15-18	10-12	6-8	6-8

При выборе времени вакуумирования также следует учитывать и возможный прирост содержания водорода при дальнейшей обработке согласно технологии на данную марку стали. Поэтому стоит задуматься и о минимизации обработки расплава после вакуумирования.

Таким образом, уменьшение затрат ресурса оборудования повлечёт за собой сокращение затрат на энергоресурсы, на компонующие материалы (футеровка, масса и др.), увеличит стойкость вакууматора за счёт сокращения времени контакта с агрессивной средой расплава и улучшит другие сопутствующие технико-экономические показатели.

Список использованных источников

1. Бигеев В.А., Основы металлургического производства: учебник / В.А. Бигеев, К.Н. Вдовин., В.М. Колокольцев – Санкт-Петербург: Издательство Лань-Трейд, 2017. - 616 с.

2. https://www.dissercat.com/content/issledovanie-i-razrabotka-tekhniki-i-tekhnologii-vakuumnoi-obrabotki-stali

3. http://emchezgia.ru/vakuumnaya/5.3_udalenie_gazov_i_primesyei.php [Текст]- Вакуумирование - удаение газов и летучих примесей в металлургии

ИНФОРМАЦИЯ

Перменкова Ксения Сергеевна, курсант 1 курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Информация, первоначально — сведения, передаваемые людьми устным, письменным или другим способом с помощью условных сигналов, технических средств и т.д. С середины 20-го века информация является общенаучным понятием, включающим в себя:

- сведения, передаваемые между людьми, человеком и автоматом, автоматом и автоматом;
- сигналы в животном и растительном мире;
- признаки, передаваемые от клетки к клетке, от организма к организму;

В Доктрине информационной безопасности Российской Федерации под термином информационная безопасность понимается состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В более узком смысле, под информационной безопасностью мы будем понимать состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений .

Защита информации – комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах.

Информационная угроза – потенциальная возможность неправомерного или случайного воздействия на объект защиты, приводящая к потере, искажению или разглашению информации.

Информационная система (автоматизированная информационная система) — это совокупность технических (аппаратных) и программных средств, а также работающих с ними пользователей (персонала), обеспечивающая информационную технологию выполнения установленных функций.

Жизненный цикл информационной системы – непрерывный процесс, начинающийся с момента принятия решения о создании информационной системы и заканчивающийся в момент полного изъятия ее из эксплуатации.

Доступность информации – свойство системы обеспечивать своевременный беспрепятственный доступ правомочных (авторизованных) субъектов к интересующей их информации или осуществлять своевременный информационный обмен между ними. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность информации – свойство информации, характеризующее ее устойчивость к случайному или преднамеренному разрушению или несанкционированному изменению.

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций4)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом информационной безопасности в тех случаях, когда информация служит «руководством к действию». Рецептура лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в буквальном смысле смертельным.

Конфиденциальность информации – свойство информации быть известной и доступной только правомочным субъектам системы (пользователям, программам, процессам). Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в России на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

Неотъемлемой частью любой информационной системы является информация. По характеру ограничений (реализации) конституционных прав и свобод в информационной сфере выделяют четыре основных вида правовой (регламентированной законами) информации:

- информация с ограниченным доступом;
- информация без права ограничения;
- иная общедоступная информация (например, за деньги);
- информация, запрещенная к распространению.

Информация с ограниченным доступом делится на государственную тайну и конфиденциальную.

Конфиденциальная информация – документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой общественной деятельности. Этой информацией владеют различные учреждения, организации и отдельные индивидуумы.

Формальные средства защиты – выполняют защитные функции строго по заранее предусмотренной процедуре без участия человека.

Физические средства - механические, электрические, электромеханические, электронные, электронно-механические и тому подобные устройства и системы, которые функционируют автономно от информационных систем, создавая различного рода препятствия на пути дестабилизирующих факторов (замок на двери, жалюзи, забор, экраны).

Аппаратные средства - механические, электрические, электромеханические, электронные, электронно-механические, оптические, лазерные, радиолокационные и тому подобные устройства, встраиваемые в информационных системах или сопрягаемые с ней специально для решения задач защиты информации.

Программные средства - пакеты программ, отдельные программы или их части, используемые для решения задач защиты информации. Программные средства не требуют специальной аппаратуры, однако они ведут к снижению производительности информационных систем, требуют выделения под их нужды определенного объема ресурсов и т.п.

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

Обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

Соблюдение конфиденциальности информации ограниченного доступа;

Реализацию права на доступ к информации.

РЕАЛИЗАЦИЯ МНОГОЗАДАЧНОСТИ В СОВРЕМЕННЫХ ОС В ОВД

Поздняков Никита Игоревич, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Термин «многозадачность» или «многопроцессорная операция» относится к способности операционной системы выполнять несколько задач (квази) одновременно. В общем, процессор также предлагает поддержку аппаратных структур для этого. Различные процессы активируются попеременно с такими короткими интервалами, что возникает впечатление одновременности. Поэтому многозадачность является вариантом метода мультиплексирования с временным разделением. Если компьютер имеет несколько ядер ЦП, чтобы он мог выполнять несколько задач в режиме реального времени, это называется многопроцессорной обработкой. Оба метода используются в сочетании в современных компьютерах.

В наше время многозадачность играет огромную роль в каждой отрасли жизни, начиная от программирования до производственных отраслей. Многозадачность - это способность операционной системы выполнять несколько задач, т.е. чтобы иметь возможность выполнять несколько прикладных программ или частей прикладных программ параллельно. Программа работает на переднем плане (обработка переднего плана), т.е. то есть входные данные могут быть сделаны и выведены на экран, остальные (фоновые задачи) работают в фоновом режиме. Однако, если вы присмотритесь, программы на самом деле не запускаются одновременно, даже если это выглядит снаружи. В действительности ресурсы процессора используются поочередно отдельными приложениями, каждое в течение доли секунды. Текущее промежуточное состояние программы буферизуется после каждого доступа, так что вы можете продолжить вычисление в этот момент, когда эта программа «по очереди».

В зависимости от того, как вычислительное время распределяется между приложениями, проводится различие между кооперативной и вытесняющей многозадачностью.

Благодаря совместной многозадачности (также без вытесняющей многозадачности) операционная система не имеет полного контроля над тем, как ресурсы распределяются между отдельными прикладными программами. Проще говоря, каждая программа определяет, насколько быстро она возвращает управление операционной системе. Однако этот метод имеет серьезный недостаток: если программа не освобождает ресурсы компьютера, например, Б. из-за программной ошибки вся система выходит из строя. Происходит сбой, и все программы отменяются. Совместная многозадачность реализована во всех версиях Windows на основе DOS (Windows 3.x, 9x, ME) и в операционных системах Macintosh до Mac OS 9.1.

Благодаря вытесняющей многозадачности (также вытесняющей многозадачности) операционная система всегда полностью контролирует освобождение ресурсов. Он поочередно назначает короткий временной сегмент (временной интервал) каждой прикладной программе. Если программа сейчас неисправна, она может аварийно завершить работу, но другие приложения не будут затронуты и продолжат работать без помех. В качестве дополнительного преимущества этот метод предлагает возможность назначать различные приоритеты отдельным приложениям. Затем программе с высоким приоритетом выделяется больше периодов времени, чем программе с низким приоритетом. Большинство операционных систем работают с вытесняющей многозадачностью, включая Windows NT, Windows XP, Mac OS X, Unix, Linux и OS / 2.

Список использованных источников

1. Гордеев, Александр Владимирович. Операционные системы [Текст] : учеб. для вузов по направлению подгот. бакалавров и магистров «Информатика и вычисл. Техника» и направлению подгот. дипломир. специалистов «Информатика и вычисл. Техника» / А. В. Гордеев. - 2-е изд. - СПб.: Питер: Питер принт, 2005. - 415 с.

2. Олифер, Виктор Григорьевич. Сетевые операционные системы [Текст] : учеб. пособие для вузов по направлению подгот. дипломир. специалистов «Информатика и вычисл. техника» / В. Г. Олифер, Н. А. Олифер. - СПб.: Питер: Питер Пресс, 2007. - 538 с.

3. Столлингс, Вильям. Операционные системы [Текст] :внутрен. устройство и принципы проектирования / Вильям Столлингс; пер. с англ. - М. [и др.] : Вильямс, 2004. - 843 с.

4. Бэкон, Джин. Операционные системы [Текст] : парал. и распре дел. системы / Джин Бэкон, Тим Харрис; пер. с англ. - СПб.: Питер, 2004. - 799 с.

5. Таненбаум, Эндрю. Современные операционные системы [Текст] / Э. Таненбаум. - 2-е изд., перераб. и испр. - СПб.: Питер: Питер Пресс, 2007. - 1037 с. - (Классика computer science).

6. Карпов, Владимир Ефимович. Основы операционных систем [Текст] : курс лекций : учеб. пособие : для вузов по специальности 351400 «Прикладная информатика»/ В. Е. Карпов, К. А. Коньков; под ред. В. П. Иванникова; Интернет- ун-т информ. технологий. - М.: ИНТУИТ. ру, 2004. - 628 с.

7. Дейтел, Харви М. Операционные системы [Текст]: [в 2 т.] / Х.М. Дейтел, П.Д. Дейтел, Д.Р. Чофнес; под ред. С.М. Молявко; пер. с англ. - М.: Бином-Пресс, 2006 - Т. 1: Основы и принципы, - 2006. -1023 с.

8. Дейтел, Харви М. Операционные системы [Текст]: [в 2 т.] / Х. М. Дейтел, П. Д. Дейтел, Д. Р. Чофнес; пер. с англ. ред. С. М. Молявко. - М.: Бином; Королев: Бином-пресс, 2006 - Т. 2: Распределенные системы, сети, безопасность: переводное издание, - 2006. - 704 с.

9. Таненбаум, Эндрю. Операционные системы. Разработка и реализация / Э. С. Таненбаум, А. Вудхалл; пер. с англ. - СПб.; М.; Нижний Новгород: Питер, 2007. - 703 с.

ИССЛЕДОВАНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ЦЕЛЬЮ ОБНАРУЖЕНИЯ НЕДОКУМЕНТИРОВАННЫХ ВОЗМОЖНОСТЕЙ

Покинен Андрей Эдуардович, курсант 4-го курса
Научный руководитель Дворянкин Олег Александрович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Программное обеспечение - это набор инструкций, данных или программ, используемых для управления компьютерами и выполнения определенных задач. В отличие от аппаратного обеспечения, которое описывает физические аспекты компьютера, программное обеспечение - это общий термин, используемый для обозначения приложений, сценариев и программ, работающих на устройстве. Программное обеспечение можно рассматривать как переменную часть компьютера, а аппаратную часть - как неизменную часть.

Для успешного анализа программного обеспечения необходимо знать о том, каких видов оно бывает, для чего предназначено и как устроено изнутри.

Все программное обеспечение можно разделить на следующие категории:

1. Системное ПО
2. Утилиты
3. Прикладное ПО

Системное программное обеспечение включает в себя операционные системы и любую программу, которая поддерживает прикладное программное обеспечение, а также представляет собой среду для его работы и взаимодействия с другими приложениями и аппаратной частью.

Утилиты представляют собой небольшие полезные программы с ограниченными возможностями. Некоторые утилиты поставляются с операционными системами. Как и приложения, утилиты, как правило, устанавливаются отдельно и могут использоваться независимо от остальной части операционной системы.

Под прикладным программным обеспечением понимаются загруженные пользователем программы, которые удовлетворяют те или иные потребности. Примеры приложений включают офисные пакеты, программы для работы с базами данных, веб-браузеры, текстовые редакторы, инструменты разработки программного обеспечения, редакторы изображений и коммуникационные платформы.

Недокументированные возможности - возможности программного обеспечения, не отраженные в документации. Такой функционал может быть добавлен разработчиками в целях тестирования, дальнейшего расширения функциональности, или же в целях скрытого

контроля за пользователем. Также недокументированные возможности могут стать следствием поспешных обновлений ПО, не учтённых разработчиками.

Следует отличать скрытые от пользователя возможности приложения, приведенные в официальной сервисной документации и лицензионном соглашении от недокументированных возможностей. Недокументированные возможности обнаруживаются, обычно, в процессе обратного проектирования, но могут быть обнаружены и случайно или с помощью автоматического исследования.

В случае программного обеспечения, отдельный интерес, представляют недокументированные возможности, которые могут поставить безопасность программного обеспечения. В этом контексте обычно используются термин уязвимость. Существует четыре основных типа документации на ПО:

- проектная — обзор программного обеспечения, включающий описание рабочей среды и принципов, которые должны быть использованы при создании ПО;
- техническая — документация на код, алгоритмы, интерфейсы, API;
- пользовательская —руководства для конечных пользователей, администраторов системы и другого персонала;
- маркетинговая —совокупность рекламной информации о ПО.

Зачастую для ее составления используют генераторы документации такие как javadoc, Ndoc, Doxygen и другие (Рисунок4).

пример для генератора Javadoc

```
/**
* Validates a chess move.
*
* Use {@link #doMove(int, int, int, int)}
* to move a piece.
*
* @param theFromFile file from which a
*                    piece is being moved
* @param theFromRank rank from which a
*                    piece is being moved
* @param theToFile   file to which a piece
*                    is being moved
* @param theToRank   rank to which a piece
*                    is being moved
* @return            true if the move is
*                    valid, otherwise false
*/
boolean isValidMove(int theFromFile, int
theFromRank, int theToFile, int theToRank)
{
   ...
}
```

пример для Doxygen

```
class PyClass:
   """Documentation for a class.

   More details.
   """

   def __init__(self):
       """The constructor."""
       self._memVar = 0;
```

Стандарты разработки документации. В настоящее время действуют следующие стандарты документирования:

1. ГОСТ 19.201 (Единая система программной документации (ЕСПД);
2. ГОСТ 2.015-2013 (Единая система конструкторской документации (ЕСКД);
3. ГОСТ 34.602 (Комплекс стандартов на автоматизированные системы (КСАС).

Применяются приведенные выше стандарты в основном в разработке ПО по государственному заказу. Коммерческие компании зачастую следуют западным стандартам или же разрабатывают собственные.

Декомпиляция - это преобразование исполняемого программного кода в некоторую форму языка программирования более высокого уровня, чтобы он мог быть прочитан человеком. Декомпиляция - однин из способов обратного проектирования, который делает противоположное тому, что делает компилятор. Инструмент, который выполняет это, называется декомпилятором. Аналогичный инструмент, называемый дизассемблером, преобразует объектный код в язык ассемблера.

Декомпиляция не всегда успешна по ряду причин. Невозможно декомпилировать все программы, и данные и код трудно разделить, потому что оба они представлены аналогично в большинстве современных компьютерных систем. Имена функций и переменных обычно

не хранятся в исполняемом файле, поэтому они обычно не восстанавливаются при декомпиляции, а ведь зачастую именно благодаря им намного проще понять ход мысли разработчика. Некоторые программы могут быть разработаны, чтобы быть устойчивыми к декомпиляции с помощью защитных средств, таких как обфускация, что делает этот процесс еще более сложным.

Примеры утилит для анализа ПО:

1) .NET Reflector;
2) IDA pro;
3) Fernflower;
4) ApkTool.

ЕСЛИ НЕ ОТКРЫВАТЬ ЗАРАЖЕННЫЕ ФАЙЛЫ, ТО ПК НЕЛЬЗЯ ЗАРАЗИТЬ

Попов Максим Александрович, студент
Научный руководитель Петров Иван Сергеевич
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Это высказывание основано на устаревших сведениях, которые до сегодняшнего дня сохранились в виде полузнаний и которым верит почти 22% участников опроса. Разумеется, заражение компьютера почти всегда происходит, когда пользователи открывают опасные файлы. Однако автоматическое исполнение вредоносных файлов возможно лишь в том случае, если злоумышленники используют существующие пробелы в безопасности. В таком случае вредоносные коды активируются без открытия зараженного файла. Поэтому всегда следует исходить из того, что зараженные файлы опасны для пользователей ПК и могут исполняться независимо от действий пользователя.

Вирусом могут быть “заражены” следующие виды файлов:

- 1. **Исполняемые файлы,** т.е. файлы с расширениями имен .COM и .EXE, а также **оверлейные файлы,** загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются *файловыми* **вирусами.** Вирус в зараженных исполнимых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те файловые вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и вредить до следующей перезагрузки компьютера. А если они заразят любую программу, запускаемую из файла AUTOEXEC.BAT или CONFIG.SYS, то и при запуске с жесткого диска вирус снова начнет свою работу.
- 2. **Загрузка операционной системы** и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются *загрузочными* **вирусами** или бутовыми (от слова boot-загрузчик). Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Для заражения компьютера загрузочным вирусом достаточно иметь всего один раз зараженную дискету в дисководе А: в момент перезагрузки компьютера. При этом вирус заразит жесткий диск компьютера. И после этого при загрузке с жесткого диска компьютера будет запускаться вирус.
- 3. Вирусы, **меняющие файловую систему** на диске, обычно называемые **DIR - вирусами.** Такие вирусы прячут свое тело в некоторый участок диска (обычно - в последний кластер диска) и помечают его в таблице размещения файлов (FAT) как конец файла. Для всех .COM и .EXE- файлов, содержащихся в соответствующих элементах каталога, указатели на первый участок файла заменяются ссылкой на участок диска, содержащий вирус, а правильный указатель в закодированном виде прячется в неиспользуемой части элемента каталога. Поэтому при запуске любой программы в память загружается вирус, после чего он остается в памяти резидентно, подключается к программам DOS для обработки файлов на диске и при всех обращениях к элементам каталога выдает правильные ссылки.
- При анализе на “чистом” компьютере с помощью программ ChkDsk или NDD файловая система зараженного DIR-вирусом диска кажется совершенно испорченной. Так, программа ChkDsk выдает кучу сообщений о пересечениях файлов и о цепочках потерянных кластеров. Не следует исправлять эти ошибки программами ChkDsk или NDD при этом диск окажется безнадежно испорченным. Для исправления зараженных этими вирусами дисков надо использовать только специальные антивирусные программы (например, последние версии Aidstest).
- 4. **Драйверы устройств,** т.е. файлы, указываемые в приложении Devise файла CONFIG.SYS. Вирус, находящийся в них, начинает свою работу при каждом обращении к соответствующему устройству. Вирусы, заражающие драйверы устройств, очень мало распространены, поскольку драйверы редко переписывают с одного компьютера на другой.

- 5. **Системные файлы DOS (MSDOS.SYS и IO.SYS)** - их заражение возможно так называемыми вирусами семейства ЗАРАЗА, так как первый из них выводил сообщение: В BOOT СЕКТОРЕ - ЗАРАЗА!. Вирус этого семейства делает следующее:
- - копирует содержимое файла IO.SYS в конец логического диска;
- - сдвигает элементы корневого каталога, начиная с третьего, на один элемент к концу каталога;
- - копирует первый элемент корневого каталога (соответствующий файлу IO.SYS) в освободившийся третий элемент корневого каталога и устанавливает в нем номер начального кластера, указывающий на место, куда было скопировано содержимое файла IO.SYS;
- - записывает свое тело в место, где находится файл IO.SYS (как правило, в начале области данных логического диска): у первого элемента корневого каталога диска устанавливает признак “метка тома”.

В результате в корневом каталоге появятся два системных файла IO.SYS. При этом система перестанет загружаться с жесткого диска, так как вирус в своем теле хранит адрес начального сектора исходного файла IO.SYS.

- 5. **Командные файлы** - заражаются достаточно редко. Обычно эти вирусы формируют с помощью команд командного файла (команд ECHO и др.) исполняемый файл на диске (как правило, в формате .COM), запускают этот файл, он выполняет размножение вируса и вредящие действия, после чего данный файл стирается. Вирус в зараженных командных файлах начинает свою работу при выполнении командного файла, в котором он находится. Иногда вызов зараженного командного файла вставляется в файл Autoexec.bat.
- 6. **Документы Word для Windows.** Так как сейчас редакторы Word для Windows более всего распространены, то в 1995 г. появилась новая разновидность вируса, заражающая файлы документов, созданные этими редакторами - **макровирусы.** Это стало возможным, поскольку в Word для Windows встроен мощный язык макрокоманд WordBasic. При этом макрокоманды не видны в редактируемом документе - для их просмотра и редактирования надо выбрать в группе меню Tools (Сервис) пункт Macro

(Макрос), а много ли пользователей вообще что-то слышали об этом пункте меню... Возможности WordBasic позволяют писать на нем вирусы. Запуск вируса происходит при открытии на редактирование зараженных документов. При этом макрокоманды вируса записываются в глобальный шаблон NORMAL.DOT, так что при новых сеансах работы с Word для Windows вирус будет автоматически активирован. При наличии вируса при сохранении редактируемых документов или записи документов или записи документов на диск под новым именем (командой Save As) вирус копирует свои макрокоманды в записываемый на диск документ, так что тот оказывается зараженным.

В принципе, возможно заражение и других объектов, содержащих программы в какой либо форме - текстов программ, электронных таблиц и т.д. Электронные таблицы содержат макрокоманды, в том числе и макрокоманды, автоматически выполняющиеся при открытии таблицы. Поэтому они могут содержать вирусы. Подобные вирусы обнаружены в табличном процессоре Excel.

Как правило, каждая конкретная разновидность вируса может заражать только один или два типа файлов. Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают только .COM-файлы, некоторые - только .EXE-файлы, а большинство - и те и другие. На втором месте по распространенности загрузочные вирусы. Некоторые вирусы заражают и файлы, и загрузочные области дисков. Вирусы, заражающие драйверы устройств, встречаются крайне редко, обычно такие вирусы умеют заражать и исполнимые файлы.

Что вирус не может заразить? Вирус является программой, поэтому объекты, не содержащие программ и не подлежащие преобразованию в программы, не могут быть заражены вирусом. Например, графические файлы форматов .BMP, .PCX, GIF, WMF и др. содержат только описания рисунков, поэтому как бы их вирус не изменял, при просмотре

или другом использовании графического файла можно получить искаженный рисунок или сообщение о неправильном формате файла, но вирус при этом не может быть запущен. Таким образом, не содержащие программы объекты вирус может только испортить, но не заразить. К числу таких объектов относятся текстовые файлы (кроме командных файлов и текстов программ), документы простых текстовых редакторов документов типа ЛЕКСИКОНа или Multi-Edit, информационные файлы баз данных и т.д.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Это “невидимые” и самомо- дифицирующиеся вирусы.

МОДЕРНИЗАЦИЯ ПОДСИСТЕМЫ УПРАВЛЕНИЯ МЕРНОГО ПОРЕЗА СЛИТКА МНЛЗ ЭСПЦ АО «ОЭМК ИМ. А.А. УГАРОВА»

Постельняк Юлия Александровна, студентка 4-го курса
Научный руководитель Азарова Виктория Сергеевна, преподаватель первой категории
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО
«Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

За последние десятилетия процесс непрерывной отливки стальных заготовок находит широкое применение в черной металлургии. Одной из главных задач, решаемых при проектировании МНЛЗ, должно быть - увеличение выхода годного металла и автоматизация всех технологических процессов, связанных с выпуском металла.

В связи с этим, весьма актуальной задачей для обеспечения непрерывности литья заготовки, является порез слитка на мерные длины. Причём, на сегодняшний день предъявляются высокие требования не только к качеству металла, но также и к таким параметрам - как длина заготовки, что в свою очередь увеличивает требования при реализации мерного пореза слитка.

В ходе оптимизации процесса пореза на мерные длины должны учитываться такие дефекты, как пояса, которые характерные для непрерывно литой заготовки. Пояса образуются в результате прекращения на некоторое время подачи металла в кристаллизатор [1].

Целью исследования является расширенный анализ подсистемы управления мерного пореза МНЛЗ.

Задачи исследования:

- представить краткую характеристику технологического процесса машины непрерывного литья заготовок;
- произвести анализ существующего уровня автоматизации подсистемы управления мерным порезом слитка;
- выявить недостатки существующей системы управления;
- опередить задачи на модернизацию системы.

Объект исследования – машина непрерывного литья заготовок ЭСПЦ АО «ОЭМК»

Предмет исследования подсистема управления мерным порезом слитка МНЛЗ АО «ОЭМК».

Принцип непрерывной разливки стали заключается в том, что жидкую сталь из ковша заливают в интенсивно охлаждаемую сквозную форму прямоугольного или квадратного сечения – кристаллизатор, где происходит частичное затвердевание непрерывно вытягиваемого слитка, дальнейшее его затвердевание происходит при прохождении зоны вторичного охлаждения. Процесс непрерывного литья позволяет получать заготовки (после резки) для прокатных станов.

Машина непрерывного литья заготовок предназначена для получения из жидкого металла заготовок сечением 300Х360мм. По конструкции МНЛЗ – радиальная, четырехручьевая с изгибом слитка в твёрдой фазе [2].

Тянуще-правильная машина (ТПМ) предназначена для вытягивания затравки вместе со слитком.

Кристаллизатор предназначен для начальной кристаллизации жидкого металла по периметру и формирования слитка требуемого размера.

Затравка предназначена для подачи непрерывно-литого слитка от кристаллизатора к тянуще - правильной машине.

Тянуще - правильная машина обеспечивает ввод затравки перед разливкой и подачу непрерывно-литой заготовки к машине газовой резки во время разливки со скоростью не более 3000 мм/мин.

Устройство хранения затравки служит для отделения затравки от головной части слитка и удержании ее в нерабочем положении в ходе разливки и в межразливочный период времени.

Секции рольгангов обеспечивают перемещение слитка.

Машина газовой резки представляет собой подвижную тележку, перемещаемую оператором вдоль ручья. Водоохлаждаемая газокислородная горелка, установленная на тележке служит для разрезания непрерывнолитой заготовки. Для синхронного перемещения тележки и слитка во время реза, тележка снабжена двумя парами пневматических захватов.

Бункер предназначен для приема технологической обрези, образующейся в ходе технологического процесса.

Объектом управления АСУ ТП мерным порезом непрерывно-литой заготовки является машина газовой резки. Объект управления функционирует в составе УНРС ЭСПЦ ОЭМК. Подсистема (УМПС) предназначена для управления технологическим процессом пореза непрерывно-литой заготовки на машинах газовой резки УНРС.

Основополагающими величинами в подсистеме УМПС, вокруг которых строится все алгоритмическое обеспечение, являются общая и текущая длины слитка.

Единственными источниками информации о движении слитков по ручью, в УМПС в настоящее время являются установленные на валу прижима ТПМ датчики типа ПДФ-5 с заданным количеством импульсов, генерируемых за один оборот вала датчика. Кроме указанной выше импульсной последовательности в подсистеме УМПС используются дискретные входные и выходные сигналы.

В результате анализа исходного уровня автоматизации было выявлено, что подсистема управления мерным порезом слитка относится к классу подсистем локальной автоматики для управления непрерывно-дискретным технологическим процессом в управляющем и информационном режиме, обладает малой информационной мощностью и средним уровнем надежности.

Управление мерным порезом слитка осуществляется на трёх УНРС с помощью мини ЭВМ СМ1420, и лишь на одной УНРС с помощью контроллера «ЭК-2000», на основе накопления общей и текущей длины слитка. Исходной информацией для накопления длины слитка является импульсная последовательность, получаемая контроллером с датчика ПДФ-5. Фотоэлектрический импульсный датчик линейного перемещения ПДФ-5 представляет собой простейший вариант дискретного измерителя, преобразуя перемещение в последовательность электрических импульсов, число которых прямо пропорционально перемещению.

Действие преобразователя основано на прохождении светового потока через два стеклянных растровых элемента, одним из которых является вращающийся диск, а другим – неподвижный сектор. При вращении вала преобразователя растровые сопряжения изменяют поступающий на фотодиоды световой поток, а фотодиоды преобразуют его в электрический сигнал квазисинусоидальной формы. Затем сигнал поступает на усилитель и формирователь, и на выходе получается сигнал в виде прямоугольных импульсов [5].

Определение момента выдачи команды на рез является одной из важнейших задач подсистемы УМПС. Принятие решения о выдаче команды "РЕЗ" зависит от следующих параметров:

- состояние входного сигнала "РУЧНОЙ/АВТОМАТИЧЕСКИЙ"
- состояние входного сигнала "ИСХОДНОЕ ПОЛОЖЕНИЕ";
- текущая длина заготовки;
- прогнозируемое приращение заготовки за время сведения захватов;
- режим предыдущего реза.

Анализируя работу УМПС и её функции можно отметить ряд существенных недостатков:

- Подсистема не имеет информации о текущей длине слитка и поэтому лишена возможности гарантировать точность пореза в режиме «ручной».

- Команда на «РЕЗ» выдаётся тогда, когда тележка резака МГР возвратилась и находится в нулевом положении – в следствии чего становится невозможным вырезать в режиме «автоматический» такой дефект как «пояс», т.к. приходится в ручную подгонять тележку резака к месту предполагаемого реза. Это в свою очередь может привести к несоответствию длины отрезаемого пояса со значением указанным в технической документации.

- Подсистемой учитывается режим реза предыдущей заготовки, поскольку, если предыдущая заготовка резалась не из исходного положения и вручную, то подсистема не имеет возможности прогнозировать положение фронтального торца заготовки, а отсюда не представляется возможным отследить общую и текущую длину слитка, а также рассчитать момент выдачи команды на рез.

- Подсистема фиксирует наличие поясов в ручье, т.е. количество остановок ручья, но никак не фиксирует длину пояса, без этой величины не возможна реализация режима «автоматический». Т.е. необходимо создание базы данных длин поясов.

- При расчёте мерных длин на замену погружного стакана подсистема мерного пореза слитка не учитывает длину пояса, который образуется после перекрывания шиберного затвора. В этом случае оператору УНРС необходимо самому подсчитать мерную длину, учитывая величину пояса исходя из технической документации.

- Аналогично и для случая, когда в ручье уже есть хотя бы один пояс, но в этом случае оператору необходимо ещё учитывать длину последнего пояса.

Целью модернизации подсистемы УМПС является обеспечение максимального выхода годных заготовок при заданных технических показателях. Управление мерным порезом слитка обеспечивает рациональное использование сырья, материалов, энергоресурсов и оборудования, а также снижение брака. В качестве главной задачи управления принят максимум точности пореза заготовки выхода годного металла.

В процессе модернизации в подсистему УМПС добавятся ряд информационных и управляющих функций:

- новая подсистема УМПС будет обладать полной информацией о таких дефектах слитка как пояса, причём удаление поясов будет в автоматическом режиме,

- в результате внедрения датчика текущей длины на тележке МГР, подсистема УМПС будет гарантировать точность реза в любом режиме,

- расчёт мерной на замену стакана модернизированная подсистема УМПС будет производить без участия оператора и оптимизация раскроя слитка от торца до пояса.

Для разработки модернизированной подсистемы управления мерным порезом слитка необходимо:

- выбрать и обосновать выбор датчика момента количества движения, который необходимо установить на МГР для того, чтобы иметь оперативную информацию о текущей длине слитка во время функционирования подсистемы УМПС [3];

- разработать новый алгоритм расчёта мерной на замену погружного стакана с учётом длины пояса, извлекаемой из базы данных;

- разработать алгоритм автоматизированного управления удаления поясов из слитка, используя список поясов и данные датчика момента количества движения;

- разработать алгоритм прогнозирования положения фронтального торца заготовки в том случае, когда рез был произведен не из исходного положения тележки МГР [4].

В результате комплексной модернизации подсистемы управления мерным порезом слитка на каждой из четырех УНРС, повысится максимальный выход годных заготовок, кроме того, новая подсистема будет заниматься не только осуществлением технологического процесса мерного пореза, но также и его оптимизацией.

Список использованных источников

1. Иванов, А. А. Автоматизация технологических процессов и производств. Учебное пособие / А.А. Иванов. - М.: Форум, Инфра-М, 2015. - 224 с

2. Клюев А.С., Лебедев А.Т. Наладка средств автоматизации и автоматических систем регулирования. Справочное пособие - М.: Энергоатомиздат, 2016 - 368с.

3. Котов К.И. Шершевер М.А. Средства измерения, контроля и автоматизации технологических процессов. Вычислительная и микропроцессорная техника. / К.И. Котов, М.А Шершевер. - М.: Металлургия, 2016. - 213 с.

4. Щагин А.В. Основы автоматизации технологических процессов: Учебное пособие для СПО / А.В. Щагин, В.И. Демкин, В.Ю. Кононов, А. Кабанова. - Люберцы: Юрайт, 2016. - 57 с.

5. Оскольский электрометалургический комбинат [Электронный ресурс] www.metalloinvest.com

БОЛЬШИНСТВО ВРЕДОНОСНЫХ ПРОГРАММ РАСПРОСТРАНЯЕТСЯ ЧЕРЕЗ USB-НАКОПИТЕЛИ

Прокопьев Кирилл Александрович студент 1-ого курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В последние годы популярность флешек и других съемных USB-накопителей значительно возросла среди кибер-преступников. Здесь используются функции автозапуска носителя данных для исполнения вредоносных программ при его подсоединении к ПК. Самым ярким примером является червь Conficker. Поэтому настоятельно рекомендуется отключить функцию автоматического запуска файлов операционной системой. Таким образом можно предотвратить автоматическую установку червя компьютером при подсоединении USB-накопителя.

В отличие от вирусов, червям для распространения не требует вмешательства человека: они заражают компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы, и затем процесс начинается снова.

Краткая история зловредных USB-устройств

Кибероружие в виде USB-устройств появилось довольно давно, первые модели увидели свет еще в 2010 году. В них была небольшая программируемая плата Teensy со стандартным USB-разъемом. Они могли имитировать работу HID-устройства (например, клавиатуры). Злоумышленники быстро сообразили, что такие устройства можно использовать для проникновения: они разработали версию, которая умела создавать новых пользователей в системе, запускать программы с бэкдорами и загружать в систему вредоносное ПО, копируя его с устройства или скачивая с сайта.

Первая модификация Teensy получила название PHUKD. За ней последовала Kautilya, совместимая с большинством популярных плат Arduino. Позже появился Rubberducky — пожалуй, самый известный USB-эмулятор нажатий клавиш (скажем спасибо *Mr. Robot*), выглядевший как обычная флешка. Более мощное устройство под названием Bash Bunny использовалось для атак на банкоматы.

Изобретатель PHUKD не остановился на достигнутом и создал «троянскую мышь», встроив в нее плату для тестирования системы на проникновение. Это с виду обычное периферийное устройство умело делать все, на что был способен PHUKD. С точки зрения социальной инженерии использовать HID-устройства для вторжения в систему может быть даже проще, чем пытаться делать это с помощью USB-флешек. Даже человек, который знает о том, что неизвестную флешку в компьютер вставлять не стоит, вряд ли задумается об опасности подключения клавиатуры или мыши.

Второе поколение вредоносных USB-устройств было создано в 2014–2015 годах — среди них, в частности, печально известные решения на базе BadUSB. Еще заслуживают упоминания TURNIPSCHOOL и Cottonmouth, которые, возможно, были разработаны Агентством национальной безопасности США. Эти устройства были настолько крохотными, что запросто помещались внутри USB-кабеля. С их помощью можно было добыть данные даже из компьютеров, которые не были подключены ни к каким сетям. Это же самый обычный кабель — кто заподозрит неладное?

Как сейчас обстоят дела со зловредными USB-устройствами

Третье поколение USB-устройств, тестирующих системы на проникновение, — это уже совершенно другой уровень. Один из таких инструментов — WHID Injector. По сути, это

Rubberducky с возможностью удаленного подключения. Благодаря поддержке Wi-Fi его уже не надо заранее программировать на определенный род деятельности: преступник может управлять устройством дистанционно, что дает ему возможность действовать по ситуации и работать в разных операционных системах. Еще один инструмент третьего поколения — P4wnP1, основанный на Raspberry Pi, модификация Bash Bunny с дополнительными функциями, включая беспроводное подключение.

Разумеется, и WHID Injector, и Bash Bunny достаточно компактны и легко помещаются в клавиатуру или мышь. На этом видеоролике показан ноутбук, который не подключен к Интернету ни по локальной сети, ни через Wi-Fi, но к нему подсоединена клавиатура с трояном, которая позволяет атакующему удаленно выполнять команды и запускать приложения.

Миниатюрные USB-устройства вроде тех, о которых мы говорили выше, можно запрограммировать так, чтобы они выдавали себя за определенную модель HID-устройства. Так можно обходить политики безопасности в компаниях, где требуют использовать мыши и клавиатуры только определенных производителей. В инструментах вроде WHID Injector также может быть микрофон, который используется для прослушки и наблюдения за сотрудниками. Одного такого устройства может быть достаточно, чтобы скомпрометировать всю сеть целиком, если она не сегментирована надлежащим образом.

ИНТЕРНЕТ КАК ИНФОРМАЦИОННО ТЕЛЕ-КОММУНИКАЦИОННАЯ ТЕХНОЛОГИЯ

Рябов Илья Игоревич, Пузаков Артём Валерьевич курсанты 2-го курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Информатизация современного общества и тесно связанная с ней информатизация образования характеризуются совершенствованием и массовым распространением информационных и телекоммуникационных технологий. Они широко применяются для передачи информации и обеспечения взаимодействия преподавателя и обучаемого в современной системе образования. Важно понимать, что в связи с этим преподаватель в наше время должен не только обладать знаниями в области информационных и телекоммуникационных технологий, но и быть специалистом по их применению в своей профессиональной деятельности.

Информационные и телекоммуникационные технологии – это обобщающее понятие, описывающее различные методы, способы и алгоритмы сбора, хранения, обработки, представления и передачи информации.

В телекоммуникационной сети Интернет доступны и многие другие распространенные сервисы, позволяющие людям общаться и обмениваться необходимой информацией, к числу которых относятся электронная почта, ICQ, списки рассылки, группы новостей, чат. Разработаны специальные программы для общения в реальном режиме времени, позволяющие после установления связи передавать тексты, звуки и изображения. Эти программы позволяют организовать совместную работу удаленных пользователей с программой, запущенной на отдельном компьютере.

Интернет – наиболее распространенный вид телекоммуникационных технологий, при которых подключение к сети может осуществляться как проводным, так и беспроводным способом. Возникновению Интернета предшествовало появление телеграфа, телефона, радио, телевидения, компьютера. Творческое объединение достоинств этих технических средств привело в конечном итоге к созданию новой технологии хранения, передачи и использования информации. Природа сети Интернет вытекает из познавательной и коммуникативной функций человеческой деятельности. Информация в форме знания в процессе познания и информационная деятельность в коммуникативном процессе как форма информационного взаимодействия находятся в тесной взаимозависимости.

С точки зрения научно-технического развития появление сети Интернет - это событие огромной важности. Современному человеку и в его преобразовательной (научной, образовательной и производственной) деятельности, и в быту уже трудно обходиться без Интернета. Очень большое значение сеть Интернет имеет и для юристов, так как она содержит огромный массив правовой и иной (связанной с правом) информации, в том числе:

– о государственных органах;

– юридической деятельности;

– международных аспектах существования и развития правовой системы;

– нормативную правовую информацию;

– судебную практику;

– правовую литературу;

– информацию о международных аспектах существования и развития правовой системы;

– новостные, статистические, аналитические материалы правового характера;

– контрправовую информацию.

Массовость. По мнению специалистов, в настоящее время число подключенных к Интернету компьютеров превысило 800 млн. Следует заметить, что количество компьютеров

и число их пользователей может не совпадать, так как один человек может иметь несколько подключенных к сети компьютеров. В нашей стране количество подключений уже составляет больше 40 млн. Пользователями Интернета становится все большее число представителей науки и образования, для которых существуют льготные условия коллективного подключения, а также целые системы (университетские коллективные компьютерные сети, академическая научная сеть, отдельные образовательные сети и т.д.).

Доступность. Интернет-сеть достаточно демократична. Для подключения к сети достаточно:

– купить средний по техническим характеристикам компьютер,

– установить на него стандартное программное обеспечение,

– позвонить провайдеру, предоставляющему интернет-услуги и заключить договор на подключение и обслуживание.

Это несложно и доступно многим. Таким образом, вы становитесь пользователем глобального сетевого информационного пространства. Условия пользования просты, а объем получаемой информации практически неограничен. Повышенная ресурсоемкость и открытость информации. Объем полезной информации в сети Интернет сегодня измеряется в сотнях экзабайт, т.е. 1018 байт. Специалисты указывают, что каждые три - четыре года количество информации в Интернете удваивается.

Сетевая информация носит открытый (транспарентный) характер. Это общий принцип деятельности в сети Интернет и распространения в ней информации. Это, безусловно, прогрессивное свойство нового для человечества технологического инструмента постепенно становится и бременем для общества, поскольку соотношение между свободой распространения информации и ответственностью ее распространителя находится в глубоком кризисе.

Телефонная линия связи (электросвязи) представляет собой физическую среду, по которой осуществляется передача сетевой информации (передача данных) между конечным телекоммуникационным оборудованием (терминалами). В зависимости от характера линии связи, принципа ее построения, назначения и использования различают линии проводной, оптоволоконной, радио-, телефонной, телеграфной и компьютерной связи. Канал сети связи (передачи данных) входит часть сети Интернет и соединяет (связывает) между собой каждую пару оконечных устройств (терминалов) связи. Коммутируемая линия связи (dial-up line) - линия связи, устанавливаемая только на время соединения передающего и принимающего коммутирующего устройства, организуемая в телефонной сети с помощью модемов (модуляторов), преобразующих аналоговый сигнал в цифровую форму (для обработки его средствами ЭВМ) и обратно.Кроме модемов в состав сложного телекоммуникационного оборудования может входить концентратор (устройство для подключения к сети Интернет нескольких рабочих станций локальной вычислительной сети) и маршрутизатор (устройство для организации связи между несколькими сетями и их взаимодействия).

Кроме того, в состав сетевой технологической инфраструктуры включены организационно-технологические требования, специально созданные для одновременной передачи данных - стандартные правила организации приема/ передачи и использования данных (протоколы TCP/IP). Протокол TCP (Transmission Control Protocol) определяет порядок разделения данных на дискретные пакеты и контролирует их передачу (доставку) и целостность. Протокол IP (Inernet Protocol) описывает формат пакета данных, передаваемых в сети, а также присвоения и поддержки адресов абонентов сети (21, 500).К организационно-технологическим элементам также относится иерархически распределенная система регистрации и идентификации сетевых компьютеров (domain name sistem). В сети Интернет существует двойное значение адресного (доменного) имени (domain name) - цифровое и символьное. Цифровое значение определяется сочетанием четырех наборов чисел (от 0 до 225), разделяемых точкой. Символьное значение определяется смысловым сочетанием букв англоязычного алфавита, например, usla.ru, yandex.ru или kremlin.ru.

Каждый компьютер в сети Интернет должен иметь свой IP-адрес - уникальное сочетание цифрового и символьного значения места его расположения в глобальной сети.К технологическим элементам сетевой инфраструктуры относится веб-браузер - специальная программа, предназначенная для просмотра страниц сети. Такая программа (например, Internet Explorer) устанавливается на компьютере пользователя сети.Кроме того, к технологическим элементам сетевой технологической инфраструктуры относится программа интеграции сетевых документов, использующая специальные языки создания и представления, а также поиска и использования документов, логически связанных между собой ключевыми словами и словосочетаниями, и обеспечивающая их быстрый поиск и просмотр (гипертекст). Такие программы используют, например, языки разметки HTML, XML и др. На основе принципов функционирования и использования этих элементов инфраструктуры организована современная система создания и представления информации в сети Интернет (WWW - World Wide Web). С этой аббревиатурой связаны различные названия элементов сети Интернет (веб-сервер, веб-портал, веб-сайт, веб-страница, веб-клиент и др.).

Наконец, к технологическим элементам сетевой инфраструктуры относится портал (сайт, страница) - технологическая информационно-телекоммуникационная система размещения, представления и использования сетевой информации, а также прямого доступа пользователей к ней. Портал (от лат. porta - ворота) представляет собой систему сетевых иерархически построенных информационных ресурсов и технологию обеспечения доступа к ним с помощью специального сервиса, программного обеспечения. Портал (сайт) может быть творчески оформленным информационным графическим рисунком, имеющим индивидуальные признаки произведения. На основании сочетания всех названных признаков (иерархия ресурсов, технология размещения, представления и использования, а также графическое оформление) портал или сайт может быть зарегистрирован как объект защиты авторского права.

РОЛЬ ОРГАНОВ ВНУТРЕННИХ ДЕЛ В СИСТЕМЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Пырх Дарья Сергеевна, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В современном мире критически важным государственным ресурсом, обеспечивающим национальную безопасность, становится информация, участвующая в телекоммуникационных и компьютерных системах различного назначения. Эти системы являются неотъемлемым компонентом структуры управления государством и обороной. Возможность воздействия на них противостоящей стороной может рассматриваться как прямая угроза национальным интересам. Навки и возможности людей в информационных технологиях уже давно вышли на первый план, поэтому теперь это одно из самых главных требований к любому нынешнему сотруднику.

Этот развития общества характеризуется рядом особенностей, к которым следует отнести, прежде всего: возросшую значимость интеллектуального труда, ориентированного на использование информационного ресурса глобального масштаба; потребность в осуществлении доступной и оперативной коммуникации между отдельными специалистами и творческими коллективами для решения совместных научно-исследовательских задач и работы над едиными проектами; интегративный характер процессов, охватывающих науку, технику, образование. Эти особенности современного социума характеризуются процессом информатизации, сущность которого заключается в непрерывном повышении уровня как профессиональной, так и информационной компетентности каждого специалиста.

Возрастающий объем различных видов информации заставляет внедрять новые, более усовершенствованные методы и средства ее обработки, а современные условия жизни предъявляют все более высокие требования к способам ее хранения, передачи, обеспечения ее безопасности.Область информационно-коммуникационных технологий позволяет осуществлять процессы сбора, хранения, передачи и использования различной информации, способов ее обработки, доставки, получения и использования.

Особое внимание уделяется деятельности МВД России в данном направлении. Россия в течение продолжительного времени объявляла о необходимости международного сотрудничества по вопросам обеспечения режима международной информационной безопасности. На сегодняшний момент Россия является один из х инициаторов развития и продвижения норм и правил информационной безопасности, используя двусторонние переговоры с другими государствами, а также региональные и международные интеграционные объединения.

Применительно к киберпреступности оказываются неэффективными традиционные методы и способы борьбы с преступностью, основанные на территориальном принципе, поскольку кибер- пространство имеет глобальный, международный характер. Эта борьба оказывается более эффективной на региональном уровне. Это объясняется существованием следующего парадокса: с одной стороны, государства вынуждены сотрудничать для борьбы с такой транснациональной угрозой, как киберпреступность, но, с другой стороны, такое сотрудничество затрагивает суверенитет государства , ограничивает его в области уголовного права и защиты информации. Поэтому сотрудничество оказывается успешным в регионах с высоким уровнем политического доверия между странами, как это происходит в Европейском союзе.

Международный характер преступности в информационной сфере требует объединенных усилий государств по ее предупреждению и противодействию. Деятельность в области борьбы с киберпреступлениями выполняется органами НЦБ Интерпола, центральными из которых являются Генеральная Ассамблея и Исполнительный комитет, чьи решения реализовываются Генеральным секретариатом, который в свою очередь определяет

свои действия с международными и национальными органами, а также выполняет функции администратора банков данных Интерпола, обеспечивающих должное качество хранящихся данных и исполнение политики доступа, которые должны соответствовать основным нормативным актам организации Интерпол. Но вопросы, которые связаны с расследованием преступлений (в том числе розыском преступника), остаются за национальным центральным бюро (НЦБ).

В 2001 г. Совет Европы принял Конвенцию о киберпреступности, представляющую собой единственный документ обязательного применения, который регулирует правоотношения в области эксплуатации компьютерной сети. Данная Конвенция весьма значима не только в рамках Совета Европы , но и на глобальном уровне. Она является одним из основополагающих документов в сфере противодействия киберпреступности. Конвенцию подписали не только страны Европы, но также Аргентина,, Австралия, Израиль, Япония, США, в общей сложности более 50 государств.

Тем не менее Россия не участвует в данной Конвенции. По мнению противников присоединения нашей страны к Конвенции, ст. 32 Конвенции противоречит российскому законодательству и нарушает суверенитет государства, так как предусмотренные в ней действия могут совершать без предварительного уведомления и согласия стороны, на территории которой эти действия совершаются.

В 1996 году Президент РФ подписал распоряжение «Об участии Российской Федерации в деятельности Международной организации уголовной полиции — Интерпола». В 1999 году в России вступил в силу указ МВД, на основе которого филиалы данной организации были созданы по всей стране. По законодательству РФ НЦБ является структурным подразделением Министерства внутренних дел и обеспечивает взаимодействие полиции и других государственных органов с Интерполом, Генеральным секретариатом и правоохранительными структурами других стран.

НЦБ является одновременно органами государства, которым присвоены полномочия по борьбе с преступностью, а также действующим органом Интерпола.

Началом правового регулирования в области киберпреступлений была Парижская конференция 1979 года, в докладе о мошенничестве которой в сфере информационной безопасности было выделено: «компьютерное преступление имеет международную природу, что является следствием устойчивого роста коммуникаций, осуществляемых с помощью телефонов, спутников и т.д., между различными странами. Международные организации, такие как Интерпол, должны уделять этому аспекту больше внимания». Но по итогам проведенной конференции были обнаружены области, нормативного регулирования для которых в то время не было.

На сегодняшний момент в Интерполе функциями каналов служебной системы наделены глобальная телекоммуникационная система связи I-24/7, построенная в 2002 г. по особенностям и правилам виртуальной частной сети, и информационная система I-Link, объединяющая функциональные назначения различных служб и подсистем Интерпола. Анализ информации, поступающей в базы данных Интерпола, позволяет обеспечить эффективное сотрудничество в сферах борьбы с преступностью, которые выявляют и раскрывают последовательную коммуникацию событий международных преступлений.Группа НЦБ Интерпола со структурными подразделениями УМВД России по Белгородской области осуществляет взаимодействие в процессе розыска и идентификации лиц, выявления, предупреждения, пресечения и раскрытия преступлений, имеющих международный характер, а также по находящимся в их производстве проверочным материалам, уголовным делам и делам оперативного учета. Также работа группы НЦБ Интерпола УМВД России по Белгородской области охватывает сферы международного розыска лиц и преступлений в сфере высоких технологий.

Положение Российской Федерации в пределах рассмотрения вопросов обеспечения международной информационной безопасности заключается в наличии трех ведущих видов угроз: террористического, криминального и военно-политического.

Список использованных источник

1. **https://xn--b1aew.xn--p1ai/**
2. **https://www.mid.ru/ru/home**
3. **https://studwork.org/shop/7927-organizacionno-pravovye-osnovy-deyatelnosti-nacionalnogo-centralnogo-byuro-interpola**

ЗАДАЧА РАСПОЗНАВАНИЯ ОБРАЗОВ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ И ЕЕ АКТУАЛЬНОСТЬ

Ракшин Никита Сергеевич, курсант
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Распознавание образов — научная дисциплина, целью которой является выявление объектов по нескольким критериям или классам. Теория распознавания объектов представляет собой раздел информатики, который основывается на разработке основ и методов идентификации предметов, явлений и сигналов. Потребность в таком распознавании возникает во многих областях, начиная с машинного зрения, символьного распознавания, диагностики в медицине, распознавания речи и заканчивая узко специальными задачами. Несмотря на то, что некоторые из этих задач решаются человеком на подсознательном уровне с большой скоростью, до настоящего времени ещё не создано компьютерных программ, решающих их в столь же общем виде. В связи с этим, проблема распознавания образов получила повсеместное распространение, в том числе в области искусственного интеллекта и робототехники.

Возможность распознавания базируется на схожести подобных объектов. Несмотря на то, что все явления и предметы не похожи друг на друга, между некоторыми из них всегда можно найти сходства по тому или иному признаку.

Распознавание образов в криминалистике – это одно из перспективных направлений компьютеризации процесса расследования — разработка систем, задача которых заключается в автоматизации процессов поиска и установления личности преступника и определёния вероятных мест совершения серийных преступлений. К этой же группе задач условно можно отнести и проблему быстрой идентификации угнанных автомобилей.

Идентификация личности – Наиболее сложными автоматизированными системами считаются системы, обеспечивающие учёт и распознавание биометрических параметров человека (индивидуальных особенностей пальца, рисунка радужной оболочки глаза, голоса, лица, фигуры), например: системы идентификации голоса, дактилоскопические автоматизированные учёты (АДИС), автоматизированные системы учёта лиц по элементам внешности (АИРС) и др.

Согласно статистике, самым распространённым и важным способом идентификации личности в криминалистике до сих пор является дактилоскопия. В соответствии с законом «О государственной дактилоскопической регистрации в Российской Федерации» от 1998 г., дактилоскопической регистрации подлежат как лица, привлекавшиеся к уголовной ответственности, так и другие категории граждан, в том числе занимающиеся опасными для жизни видами деятельности (статья 9), например военнослужащие, сотрудники правоохранительных органов. Также возможно добровольное прохождение регистрации.

Автоматизация дактилоскопических учётов заключается в создании автоматизированных дактилоскопических информационных систем (АДИС) с возможностью создавать и хранить в электронном виде большие массивы дактилоскопической информации, производить по ним поиск с использованием папиллярных узоров пальцев (или ладоней) рук. Разработка АДИС состоит, прежде всего, в подготовке базы данных с дактилокартами лиц, состоящих на учёте, и следами пальцев рук и ладоней, изъятых на месте преступления. В дальнейшем, поступающие на учёт дактилокарты и следы, программа сравнивает с имеющимися в её базе. По сравнению с визуальной проверкой дактилокарт и следов экспертами, АДИС позволяют более точно и быстро идентифицировать личность.

Для автоматизации дактилоскопических учётов в России, формируемых в рамках закона «О государственной дактилоскопической регистрации в Российской Федерации», в том числе и криминалистических учётов, применяется АДИС «Папилон» (рис. 3.3). Все крупнейшие российские автоматизированные банки данных дактилоскопической

информации федерального, межрегионального и регионального уровня построены на базе АДИС «Папилон». В электронный формат «Папилон» переведены практически все бумажные дактилоскопические учёты страны. Пользователями АДИС «Папилон» в России являются подразделения Министерства внутренних дел, Федеральной службы безопасности, Федеральной службы по контролю за оборотом наркотиков, Федеральной службы исполнения наказаний, Федеральной миграционной службы и Министерства обороны.

Система «Папилон» обеспечивает создание, хранение и функционирование электронной базы данных дактилокарт и следов и автоматизацию процесса дактилоскопической идентификации для решения широкого круга задач:

1. установления личности по отпечаткам и следам пальцев рук и ладоней, в том числе путём проведения оперативных проверок по оттиску пальца в режиме реального времени;
2. идентификации неопознанных трупов;
3. установления причастности личности к ранее совершённым преступлениям;
4. объединение преступлений, совершённых одним и тем же лицом.

Система распознавания госномеров – компьютерная система, которая уже широко используется в больших городах РФ, на автомагистралях и т. д. Система позволяет считывать номера авто и выставлять на базе полученной информации штрафы за правонарушения ПДД. Система построена на аналоговой видеокамере, IP камере

Модули характеризуются наличием таких функциональных возможностей: Можно распознавать регистрационные номера машины, что движется. Данные при этом сохраняются в архивы информации о временном периоде, дате, номерах, остается также ссылка на соответствующие видеокадры. Можно перехватывать по номерам транспорт, что есть в картотеке в реальном времени. Можно отыскать автомобиль в архивах по времени, датам, номерам и дополнительным данным из картотек. Можно работать со встроенными картотеками автономеров, что позволяют добавить или изменить номерные знаки, ввести дополнительные сведения о транспорте, формировать список перехвата. Система распознавания номерных знаков авто используется, чтобы вести учет транспортных средств на въездах на охраняемые территории и для автоматизации паркинга.

Модули способны: обрабатывать видеопоток придерживаясь скорости 6 – 25 кадров в секунду; распознавать несколько номерных знаков одновременно; распознавать знаки при вертикальных углах до 40°, и горизонтальных до 30°; применять детекторы движения, чтобы уменьшить вычислительные затраты при идентификации номеров; задать отдельную поисковую область, чтобы уменьшить вычислительные затраты при идентификации; распознавать стандартный тип знаков, что соответствуют стандартам РФ, Украины, Италии и т. д.

Система распознавания решает такую задачу: распознает номера; измеряет скорость движения транспорта; детектирует дорожно-транспортные происшествия и пробки; детектирует нарушения ПДД – фиксируются моменты, когда превышено скорость, авто движется в обратных направлениях, пресекается сплошная линия и др.; определяет и классифицирует автомобили – легковой, грузовой транспорт, автобус, мотоцикл; собирает статистику транспортных потоков; собирает статистику транспортного потока; транслирует изображение в центры наблюдения.

Системы распознавания госномеров могут использоваться:

На автостоянке и паркинге – система распознавания автомобильных номеров для шлагбаума. Благодаря устройству осуществляется автоматическая регистрация факта на въезде и выезде. Не нужно оформлять парковочные талоны, а значит, исключается риск махинаций сотрудников, и повышается оперативность обслуживания. Будет также гарантировано сохранность транспорта.

На промышленном предприятии – с целью контроля въезда и выезда с территории. Исключается риск несанкционированных проездов на объект. Контролируются ввозимые и вывозимые грузы, определяется их соответствие документам. Возможна организация

дифференцированного въезда. Можно интегрировать и строить территориально распределенные решения, обеспечить надежную работу с любыми условиями.

Дорожной патрульной службой. Благодаря системе возможно обеспечение безопасности на дороге. Можно осуществлять контроль транспортного потока, выявляя авто с определенными знаками.

Муниципальными властями, чтобы организовать дифференцированный въезд в определенную городскую зону – центры, режимную и особо охраняемую зону.

В заключение нужно отметить, что большинство специалистов, как разработчиков, так и пользователей систем распознавания убеждены, что распознавание образов – одновременно и наука, и искусство. Это, в принципе, можно отнести к любому направлению, связанному с моделированием, разработкой и эксплуатацией систем искусственного интеллекта. Недаром подробное и всеобъемлющее руководство пользователя по пакету ERDAS Imagine в вопросах проектирования конкретных систем тематической обработки отправляет пользователя к опыту разработки таких систем для соответствующих прикладных направлений. Несмотря на то, что в руководстве приводятся преимущества и недостатки каждого метода классификации, все нюансы их применения могут быть выявлены только в процессе практической работы.

ИССЛЕДОВАНИЕ ЭНЕРГОЗАВИСИМОЙ ПАМЯТИ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА

Рачкинда Дмитрий Александрович, курсант 4-го курса
Научный руководитель Дворянкин Олег Александрович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Энергозависимая память персонального компьютера – временная память персонального компьютера, в которой находится важные данные. В ней хранится такая информация как, как последние посещённые веб-страницы и пароли от них, а также от других приложений, пользовательская информация, которая остаётся после использования браузера, последние подключения к удалённым серверам. И этот список не является исчерпывающим. Из этого можно сделать вывод о том, что исследование энергозависимой памяти персонального компьютера, или другого устройства очень важно для проведения судебной экспертизы, а также для того, чтобы получить доступ к системе и внутренней сети. При этом мы должны понимать, что часто, при попытке получить нужную информацию, можно столкнуться с проблемами, так как зачастую в этой памяти возникают ошибки, что делает тему работы и дальнейших исследований ещё более значимыми.

Исследование программного обеспечения, позволяющего провести выгрузку данных из энергозависимой памяти, а также анализировать полученные сведения является первоначальной задачей эксперта при проведении обучения и при непосредственном проведении экспертизы или специалиста, проводящего “исследование предметов и документов”. То есть изначально нам нужно изучить и понять, что такое энергозависимая память и как она взаимодействует с другими компонентами системы, после чего приступить к исследованию программного обеспечения, которое позволит нам получить информацию и только потом провести её анализ.

В персональном компьютере можно видеть два типа информации: энергозависимую, которая стирается при приостановке питания на неё, и энергонезависимую, которая обладает возможностью сохранять информацию на долгосрочный период даже при выключенном питании.

Оперативная память – основная память персонального компьютера, которая хранится на оперативно записывающем устройстве (ОЗУ). Она обладает сравнительно большими объёмами, в современном компьютере от 2GB до 32GB, и высокой скоростью работы, который составляет примерно 50нс, а также способностью с одинаковой скоростью обращаться к любой ячейке, поэтому оперативную память называют памятью со случайным доступом (RAM – random access memory). В данной памяти хранятся такие данные, как последние посещённые веб-страницы и пароли от них, а также от других приложений, пользовательская информация, которая остаётся после использования браузера, последние подключения к удалённым сервера и так далее, что позволяет экспертам, при проведении экспертизы получить множество полезной информации о пользователях системы, а также о их последних и частых действиях. Данные такого типа очень важны для следствия и могут играть решающую роль в уголовном деле.

Можно заметить, что существует много программного обеспечения, инструментов, которые направлены на анализ готовых снимков оперативной памяти, список не заканчивается на тех, которые рассматривались в данной работе, есть ещё Mimikatz, KnTTD, aeskeyfind и множество других не менее отличных. Данные утилиты направлены и решают свои поставленные задачи, также они могут помочь в работе как новичкам, так и профессионалам. Что позволяет любому человеку найти ряд своих “любимых” и использовать их.

Часто, пользователи считают, что если они заблокировали компьютер паролем, зашифровали диск или выполнили ещё какие-либо действия, направленные на то, чтобы обезопасить свою систему, то доступ к информации, находящейся на их персональном или

рабочем компьютере, никто получить не сможет. В итоге, рассмотрев понятия оперативной памяти, способы получения доступа к зашифрованным системам, можно понять, что в оперативной памяти, хранится достаточно большое количество информации о системе и о пользователе, его действиях, удалённых подключениях, всё-таки оперативная память – основная память компьютера, и получить доступ к ней можно достаточно большим количеством способов. Так что пользователь, если он хранит какую-либо конфиденциальную или секретную информацию на своём компьютере должен обезопасить себя от множества факторов, которые помешают злоумышленнику получить к ней доступ. Ведь если это персональный компьютер организации, можно также получить доступ в её сеть.

ИСПОЛЬЗОВАНИЕ ЗАЩИЩЕННОЙ ЛОКАЛЬНОЙ СЕТИ ДЛЯ РАБОТЫ ПРЕДПРИЯТИЙ

Ремидовская Ирина Александровна, курсант 3-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В настоящее время резко возросло количество преступлений в сфере компьютерной информации, это кражи персональных данных, распространение вредоносных программ, неправомерный доступ к компьютерной информации и другие. Как правило все эти действия выполняются удаленно и через специально созданную логическую сеть с множеством узлов, от которой путь к преступнику, зачастую, отследить невозможно. Во избежание данной проблемы предприятию следует настроить защищенную локальную сеть, с помощью которой, данные, находящиеся в обороте у предприятия не смогут подвергнуться удаленному взлому.

Государственным реестр сертифицированных средств защиты информации Федеральной службы по техническому и экспортному контролю предоставляет обширный перечень данных средств. Одним из них является программно-аппаратный комплекс ViPNet Coordinator IG 4. Данный комплекс был произведен российским разработчиком сертифицированного программного обеспечения в сфере информационной безопасности «АО ИнфоТеКС» и внесен в реестр 22 марта 2021 года.

Программно-аппаратный комплекс ViPNet Coordinator IG 4 является шлюзом безопасности, позволяющий предоставить защиту для каналов связи по технологии ViPNet VPN, а также он направлен на предотвращение от несанкционированного доступа к объектам автоматизированных систем управления (АСУ) и автоматизированным системам управления производственным и технологическим процессом (АСУ ТП). Комплекс полностью соответствует требованиям Приказа №239 ФСТЭК России от 25.12.2017 г., стандартов ГОСТ Р МЭК 62443 и позволяет реализовать различные сценарии безопасности. Данное средство защиты поддерживает такие каналы, как Ethernet, GSM/UMTS/LTE, Wi-Fi, RS-232/RS485.

ПАК ViPNet Coordinator IG предназначен для использования:

– в государственных информационных системах (ИС) до класса защищенности К1 включительно;
– в автоматизированных системах управления технологическим процессом (АСУ ТП) до класса защищенности К1 включительно;
– в информационных системах (ИС) для обеспечения 1 и 2 уровня защищенности персональных данных;
– в информационных системах (ИС), информационно-телекоммуникационных системах (ИТС) и автоматизированных системах (АСУ) критической информационной инфраструктуры (КИИ) до 1 категории значимости.

ViPNet Coordinator IG совместно с другими продуктами ViPNet Network Security предназначен для реализации следующих сценариев безопасности:

– сегментирования сети и разграничения доступа к ее сегментам;
– защиты проводных и беспроводных каналов связи сети;
– организации защищенного удаленного мониторинга;
– организации удаленного сервисного обслуживания;
– организации защищенного конфигурирования оборудования внутри сегмента сети;
– организации защищенного подключения оборудования по последовательным интерфейсам.

Преимущества:

– Защита проводных и беспроводных каналов связи.
– Работа в режиме «горячего» резервирования.

– Резервирование каналов передачи информации.

– Раздельная настройка межсетевого экрана для разных режимов работы ИС и АСУ – штатном режиме, специальном и регламентном обслуживании.

– Глубокая фильтрация промышленных протоколов.

– Предотвращение доступа к устройствам, подключенным по RS-232 и RS-485.

– Индустриальный дизайн и возможность эксплуатации в жестких климатических условиях.

– Возможность дистанционного конфигурирования и управления политиками безопасности.

– Возможность построения сквозной безопасность предприятия от ERP уровня до нижнего уровня АСУ и АСУ ТП на основе единой технологии ViPNet VPN с помощью линейки продуктов ViPNet Network Security.

Также можно рассмотреть средство защиты он несанкционированного доступа «Блокхост-Сеть 4». Данное средство является программно-техническим средством контроля съемных машинных носителей информации (СКН), предназначенным для защиты от несанкционированного доступа к информации, АС класса защищенности 1Г, ГИС 1 класса защищенности, АСУТП 1 класса защищенности, обеспечения безопасности персональных данных 1 уровня защищенности, значимых объектов КИИ 1 категории на базе персональных компьютеров (ПК) под управлением операционных систем (далее – ОС) Microsoft Windows 2008R2/7/8.1/2012/2012R2/10/2016/2019.

СЗИ от НСД «Блокхост-Сеть 4» является специализированным программно-техническим СЗИ, которое обеспечивает возможность:

– идентификации и аутентификации пользователей ИС при попытках входа на защищаемые персональные компьютеры (далее - ПК).

– двухфакторной аутентификации пользователей ИС при входе на защищаемые ПК, при помощи аппаратных (аппаратных «идентификационных носителей пользователя» с USB -интерфейсом) носителей.

– контроля прав доступа пользователей ИС к защищаемой информации на ПК.

– контроля подключения и использования съемных машинных носителей информации (МНИ) на защищаемых ПК.

СЗИ от НСД «Блокхост-Сеть 4» обеспечивает:

– пятый класс защищенности для средств вычислительной техники (СВТ) в соответствии с руководящим документом «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации», Гостехкомиссия России, 1992;

– четвертый класс защиты в соответствии с методическим документом «Профиль защиты средств контроля подключения съемных машинных носителей информации второго класса защиты ИТ.СКН.П4.ПЗ», ФСТЭК России, 2014;

– четвертый уровень контроля в соответствии с требованиями к уровням доверия и методикой для дифференциации требований к исследованиям программного обеспечения средств защиты информации по выявлению уязвимостей и недекларированных возможностей, приказ ФСТЭК России от 30 июля 2018 г. N 131

В соответствии с ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» защищенность обеспечивается тремя группами требований к средствам защиты, реализуемым в СВТ:

– Требования к разграничению доступа, предусматривающие, что СВТ должны поддерживать непротиворечивые, однозначно определенные правила разграничения доступа.

– Требования к учету, предусматривающие, что СВТ должны поддерживать регистрацию событий, имеющих отношение к защищенности информации.

– Требования к гарантиям, предусматривающие необходимость наличия в составе СВТ технических и программных механизмов, позволяющих получить гарантии, что СВТ обеспечивают выполнение требований к разграничению доступа и к учету.

Использование защищенных локальных сетей позволит обезопасить работу с документами и другими информационными материалами внутри предприятия.

Список использованных источников

1. **https://elibrary.ru/**
2. **https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty-po-sertifikatsii/153-sistema-sertifikatsii/591-gosudarstvennyj-reestr-sertifitsirovannykh-sredstv-zashchity-informatsii-n-ross-ru-0001-01bi00**
3. **https://infotecs.ru/**

БРАНДМАУЭР ЗАЩИЩАЕТ ОТ ЗАРАЖЕНИЯ

Романенко Сергей Алексеевич курсант 1 курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Этот тезис ложен. Брандмауэры – это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной Web-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных задании вредоносной программой и, например, отправку данных злоумышленникам, если речь идет о шпионских программах.

Брандмауэр & в windows Security позволяет просматривать состояние брандмауэра Microsoft Defender и сети, к каким сетям подключено устройство. Вы можете включить Microsoft Defender брандмауэра и получить доступ к дополнительным Microsoft Defender брандмауэрам для следующих типов сети:

- Доменные (рабочие) сети
- Частные сети (с обнаружением)
- Общедоступные сети (без обнаружения)

"Параметры сети"

При выборе одного из трех типов сети вы увидите страницу его параметров. Здесь служба безопасности Windows сообщает, к какой из сетей этого типа вы сейчас подключены. Обычно компьютер будет подключен только к одной сети.

Кроме того, вы найдете простой ползунок для того, чтобы отключить или отключить брандмауэр для сети этого типа.

Важно: Отключение брандмауэра может повысить риск для устройства или данных. Мы рекомендуем не выключать его, если вы абсолютно не хотите его отключать.

В разделе "Входящие подключения" вы найдете один установленный для блокировки всех входящих подключений, включая те из них, которые находятся в списке разрешенных приложений. При этом брандмауэр Защитника Майкрософт будет игнорировать список разрешенных приложений и заблокировать все. Включение этого приложения повышает уровень безопасности, но может привести к тому, что некоторые приложения перестанут работать.

На странице защиты сети брандмауэра &:

Разрешить приложение через брандмауэр. Если брандмауэр блокирует приложение, которое вам действительно нужно, вы можете добавить исключение для этого приложения или открыть определенный порт. Узнайте больше об этой процедуре (и о том, почему вы не хотите этого делать) на рисках, связанных с разрешением приложений через брандмауэр Microsoft Defender.

Устранение неполадок с сетью и Интернетом. Если у вас возникли общие проблемы с сетевым подключением, используйте его для диагностики и автоматической диагностики и исправления.

Параметры уведомлений брандмауэра: хотите получать дополнительные уведомления, когда брандмауэр блокирует что-то? Меньше?

Дополнительные параметры. Если вы хорошо знаете о параметрах брандмауэра, откроется классическое средство брандмауэра Защитник Windows, с помощью которого можно создавать правила для входящего и исходящие подключений, правила безопасности подключений и смотреть журналы мониторинга для брандмауэра. Большинству пользователей не хочется тщательно врывываться в него. Неправильное добавление,

изменение и удаление правил может привести к тому, что система станет более уязвима или некоторые приложения не будут работать.

Восстановление брандмауэров по умолчанию. Если кто-то или что-то внести изменения в параметры брандмауэра Windows, которые не работают должным образом, то сразу за два щелчка вы не сможете восстановить параметры так, как это было при первом подстановлении компьютера. Если в вашей организации настроены какие-либо политики брандмауэра, они будут повторно применены.

КТО И ЗАЧЕМ УГРОЖАЕТ РОССИИ В ИНФОРМАЦИОННОМ ПОЛЕ И ГДЕ У НЕЕ СЛАБЫЕ МЕСТА

Романов Егор Александрович, курсант
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Главной целью информационной войны, которая ведётся против России, является дестабилизация ситуации внутри страны, в частности организация «оранжевой революции» и других негативных сценариев в России, а вне страны — развитие антироссийского вектора общественного мнения сопредельных и «натовских» стран. Приоритетом является ослабление России и порча её репутации за рубежом. В частности, Запад навязчиво пытается выставить Россию «тиранической», «отсталой» и «агрессивной»: при этом агитация направлена как на население России, так и на жителей других стран.

Несмотря на превосходство противника в численности и мастерстве, ситуация складывается в целом в пользу России.

Государство хоть и медленно, но призывает к порядку принадлежащие ему СМИ. Тот факт, что против России ведётся информационная война, был, наконец, признан официально и открыто — с 26 декабря 2014 года в военной доктрине России в качестве одной из внутренних и внешних угроз названо информационное воздействие на население с целью подрыва исторических, духовных и патриотических традиций в области защиты Отечества, а также разжигание межнациональной и межрелигиозной розни.

Всё больше появляется пророссийских блогеров и общественных деятелей. У многих людей наступает передозировка русофобии: им надоедают потоки грязи, которые льются изо всех щелей на их страну. Наконец, люди становятся опытнее: после краткого периода слепой эйфории они начинают видеть нестыковки и передёргивания во вражеской агитации.

Становится всё сложнее отрицать тот факт, что против России ведётся настоящая информационная война — особенно после того, как Штаты открыто заявляют о запуске новых проектов по ведению информационной войны против России. Люди со здоровой моралью не допускают возможности принимать участие в информационной войне на стороне врагов России.

Наконец, мы находимся на своей территории, а наш противник вынужден орудовать на чужой: он плохо понимает наши реалии, и регулярно допускает из-за этого болезненные просчёты.

С 2007 по 2015 год число россиян, не доверяющих иностранным СМИ, увеличилось в 7 раз — до 50 %.

Можно уже констатировать факт: в 2014 году в информационной войне произошёл перелом в нашу пользу. Однако пока наши успехи ограничиваются преимущественно внутренним фронтом. На Западе СМИ продолжают с помощью привычных методов пропаганды и разнообразных провокаций выстраивать негативный образ России. Однако и там есть успехи: работа телеканала RT, международного информагентства Sputnik и прочих иноязычных российских СМИ впервые в истории дала западному обывателю возможность систематически знакомиться с российским взглядом на важнейшие мировые события.

Кто и зачем угрожает России в информационном поле и где у нее слабые места:

- Зарубежные СМИ увеличивают объем материалов, содержащих предвзятую оценку государственной политики России.
- Российским журналистам за рубежом мешают заниматься профессиональной деятельностью.
- Население России (а особенно — молодежь) зомбируют «в целях размывании традиционно российских духовно-нравственных ценностей».

- Террористические организации воздействуют на отдельных людей и их группа, а также на все общество, нагнетая атмосферу межнациональной и социальной напряженности, а также вербуют новых сторонников.
- Растет количество и масштабы кибератак на кредитно-финансовую сферу.
- Отдельные государства и организации применяют информационные технологии в военно-политических целях, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников
- Усиливается разведывательная деятельность иностранных государств в отношении России.

ВЫЯВЛЕНИЕ И РАССЛЕДОВАНИЕ СЛУЧАЕВ ОТМЫВАНИЯ ПРЕСТУПНЫХ ДОХОДОВ С ИСПОЛЬЗОВАНИЕМ ВИРТУАЛЬНЫХ ВАЛЮТ

Румянцев Илья Алексеевич, курсант 3-го курса
Научный руководитель Карен Рафаэлович Аветисян, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Цель этой статьи – рассказать об инструментах и методах, доступных для обнаружения и расследования отмывания доходов, полученных преступным путем, с использованием виртуальных валют.

Разделим доступные инструменты и методы на две широкие группы: законодательные инструменты и инструменты расследования.

Одна из основных целей каждого уголовного расследования – обеспечить надлежащую квалификацию предполагаемой преступной деятельности в соответствии с соответствующим уголовным законодательством, то есть определить элементы преступления. Хотя большая часть нынешней практики в отношении отмывания доходов сформирована многолетним опытом расследования, некоторые новые формы преступной деятельности - одним из таких примеров является преступное использование виртуальных валют - могут потребовать переосмысления и корректировки имеющихся в настоящее время уголовного законодательства для реальных дел, которые еще предстоит всесторонне урегулировать ни законом, ни практикой. Таким образом, цель этого части статьи - предоставить различные варианты, доступные в уголовном праве, для рассмотрения элементов преступления отмывания денег в контексте виртуальных валют.

Прежде чем приступить к рассмотрению рассматриваемых вопросов, необходимо иметь в виду текущую неоднозначность статуса виртуальных валют, и, поскольку их использование прямо не криминализируется ни в одном из государств ГУАМ (или в любом другом государстве, если на то пошло) , использование виртуальной валюты само по себе не может считаться правонарушением из-за принципа технологической нейтральности.

Отмывание денег относится к схеме финансовых транзакций, которая направлена на сокрытие личности, источника и назначения денег, полученных незаконным путем. Причины, по которым правонарушители - будь то торговцы наркотиками, корпоративные растраты или коррумпированные государственные должностные лица - используют эти механизмы, заключаются в том, чтобы скрыть незаконное происхождение соответствующего имущества или помочь любому лицу, которое причастно к совершению преступления. Предикатное преступление, направленное на уклонение от правовых последствий его или ее действий путем сокрытия или маскировки, применяемых к истинному характеру, источнику, местонахождению, расположению, перемещению или владению или правам в отношении собственности, полученной преступным путем. Другими словами, преступники пытаются отмыть средства, полученные преступным путем, чтобы скрыть доказательства своих преступлений и, во-вторых, защитить деньги, полученные незаконным путем, от ареста. Преступники все чаще пользуются преимуществами глобализации мировой экономики, быстро переводя средства через международные границы с использованием, среди прочего, информационных и коммуникационных технологий, которые позволяют деньгам легко и быстро перемещаться в любую точку мира. Независимо от того, кто использует аппарат для отмывания денег, принципы работы основаны на одном и том же трехэтапном процессе:

1. Этап размещения представляет собой первоначальный ввод средств в финансовую систему. Когда речь идет о крупных денежных суммах, это может оказаться сложной задачей, особенно если используются наличные.

2. После размещения следует расслоение, которое обычно состоит из серии транзакций, предназначенных для сокрытия происхождения средств. Это самый сложный этап процесса и самый международный по своему характеру. Лицо, занимающееся отмыванием денег, может начать с отправки средств в электронном виде из одной страны в

другую, а затем разбить их на инвестиции или на зарубежные рынки, постоянно перемещая их, чтобы избежать обнаружения, каждый раз надеясь использовать лазейки или несоответствия в законодательстве и задержки в судебном или полицейском сотрудничестве.

3. Заключительный этап отмывания денег называется этапом интеграции, потому что именно на этом этапе средства возвращаются полностью ассимилированными в легальную экономику.

Будучи изначально размещенными в виде наличных средств и расслоенными посредством ряда финансовых операций, доходы от преступной деятельности полностью интегрированы в финансовую систему и могут быть использованы для любых целей.

При нынешнем состоянии дел повестка дня по отмыванию денег с целью незаконного использования виртуальных валют становится все более актуальной в свете реальных случаев.

Несмотря на то, что существуют существенные различия в условиях работы централизованных или децентрализованных виртуальных валют, что, пожалуй, наиболее ярко показано на примерах «Silk Road» и «Liberty Reserve», анонимность, отслеживаемость или использование криптографии децентрализованных валют могут быть привлекательными вариантами. за сокрытие доходов, полученных преступным путем.

В более традиционной теории уголовного права, элементы преступления можно разделить на объективные и субъективные категории. Использование виртуальных валют для отмывания денег подчеркивает это различие. Объективные элементы преступления, связанные с использованием виртуальной валюты, технически не будут отличаться от объективных элементов любого другого преступления, включая «традиционные» преступления по отмыванию денег; использование экспертов и их экспертных заключений может быть необходимо для описания технических вопросов, относящихся к централизованным и децентрализованным виртуальным валютам, и для проведения аналогий с традиционными финансовыми транзакциями.

Вообще говоря, использование виртуальной валюты в качестве объективного элемента уголовного преступления, связанного с отмыванием денег, можно свести к следующим аспектам:

- С точки зрения размещения (когда средства, полученные преступным путем, вводятся в финансовый оборот), приобретение виртуальной валюты через обменник (в случае децентрализованных валют) или администратора (в случае централизованных валют) может использоваться в качестве соответствующего элемента. преступления;

- С точки зрения многоуровневости (процесс, в котором средства, полученные преступным путем, легализуются, а их право собственности и источник скрывается), основные характеристики виртуальной валюты (в первую очередь, анонимность и сложная отслеживаемость транзакций) могут быть выдвинуты как элемент денежного обращения. преступление отмывания денег, при котором обвинение будет готово доказать, что виртуальная валюта была выбрана именно для этих функций, чтобы скрыть преступное происхождение средств. Фактически, сосредоточение внимания на разделении на уровни с точки зрения использования виртуальной валюты, возможно, является центральным аргументом в пользу доказательства намерения;

- В части интеграции (процесс легализации собственности путем расслоения повторно вводится в экономику), использование виртуальной валюты может быть одним из элементов, в зависимости от случая: в основном, если отмытые доходы реинвестируются на рынок виртуальной валюты, это может быть дополнительным элементом о преступлении, которое может быть использовано. Что касается доказательства умысла, которое является важным признаком преступлений, связанных с отмыванием денег, ситуация будет иной. Аргументы государства можно подкрепить, снова сосредоточив внимание на наиболее важных характеристиках виртуальных валют:

- анонимность и общее отсутствие личного общения могут быть веским доказательством намерения совершить преступление, связанное с незаконным

использованием виртуальных валют, в отличие от наличия традиционных, более прозрачных и устоявшихся финансовых механизмов;

- трудность прослеживаемости, в том числе отсутствие бумажного / документального следа, может быть особо отмечена как элемент намерения, при этом может быть доказана аналогичная логика отказа от традиционных финансовых механизмов;

- в случае децентрализованных виртуальных валют, использование криптографии, что делает любой криминалистический анализ чрезвычайно трудным;

- всеобъемлющая проблема виртуальных валют с точки зрения доказательства намерений - это природа самих виртуальных валют, то есть их функционирование за пределами установленных финансовых учреждений и общее отсутствие регулирования, что может быть доказано как осознанный выбор.

Правоохранительные органы могут добиться сохранения указанных компьютерных данных в связи с конкретным уголовным расследованием или судебным разбирательством; в основном это делается с целью предотвращения удаления компьютерных данных, важных для расследования киберпреступлений. Это позволяет сохранить данные в неприкосновенности, а данные в сохраненной форме защищены от всего, что может привести к изменению или ухудшению их текущего качества и доступности. Хранение компьютерных данных позволяет оперативно сохранять указанные компьютерные данные, в частности, когда есть основания полагать, что компьютерные данные особенно уязвимы для потери или модификации (например, существует бизнес-политика по удалению данных по истечении определенного периода времени. или данные обычно удаляется, когда носитель данных используется для записи других данных, или просто данных трафика, которые хранятся в течение ограниченного времени).

Процедуры поиска и изъятия компьютерных данных, по сути, являются ассимиляционными положениями, которые направлены на гармонизацию уже существующих уголовно-процессуальных полномочий по поиску и изъятию материальных объектов с точки зрения их применения к компьютерным системам и данным. Таким образом, поиск и изъятие хранимых данных в значительной степени отличается от поиска и изъятия материального объекта, который включает в себя осмотр физического участка и удаление материального объекта из обыскиваемого помещения. В цифровой среде сбор данных происходит в период поиска и в отношении данных, существующих в то время.

В то же время природа электронных доказательств (т.е. данных, хранящихся в компьютерной системе в нематериальной цифровой форме) также может потребовать другого подхода по сравнению с традиционными процедурами поиска и изъятия. Самое главное, должна быть обеспечена читаемость данных: если данные могут быть прочитаны только компьютерной системой, в которой они хранятся, вся система должна быть конфискована; в других случаях копия данных может быть сделана и удалена на физическом запоминающем устройстве. Точно так же данные могут быть извлечены из подключенных устройств (хранилища, сети и т.д.). В этом отношении процедуры изъятия компьютерных данных, по которым производился поиск, по сути не отличаются от традиционных процедур изъятия.

С точки зрения практического применения ситуация с обыском и выемкой может быть менее ясной, чем с другими, более специализированными процессуальными полномочиями. С одной стороны, обыск и выемка в традиционном смысле могут быть предприняты любым правоохранительным органом, и, при необходимости, могут быть привлечены эксперты-специалисты для облегчения поиска и выемки. С другой стороны, удаление улик из компьютерных систем или даже удаление самих компьютерных систем из обыскиваемых помещений может потребовать передовых знаний для сохранения читабельности и целостности данных.

Цепочка хранения электронных доказательств, по сути, не отличается от цепочки хранения традиционных доказательств. Уголовное судопроизводство основывается на высоко формализованных процедурах и требованиях. Следовательно, соблюдение

установленных процедур, обеспечение обращения со стороны лиц, обладающих достаточной квалификацией для этого, и ведение документооборота, чтобы показать, когда и как доказательства были сохранены, доступны или использованы, представляют собой стандартный подход, применимый к любому уголовному процессу и к любому типу доказательств, которые могут быть использованы в таком разбирательстве. Электронные доказательства, с другой стороны, имеют некоторые дополнительные особенности, которые необходимо учитывать для обеспечения надлежащей цепочки хранения:

Целостность данных: электронные доказательства очень изменчивы. Доступ к компьютерной системе, даже для простого просмотра, в большинстве случаев изменяет данные (например, список «недавно просмотренных» документов) до такой степени, что это не может быть использовано в качестве доказательства в уголовном процессе. Следовательно, компьютерные данные должны быть всегда защищены от возможных модификаций, а ряд методов и методов (таких как доступ только в «режиме чтения», изучение цифровой копии, а не «оригинала» доказательства, отображение или запись обработки и т.д.) используется для сохранения подлинности данных.

Контрольный след: очень важно отслеживать официальные документы, сопровождающие процесс расследования. В уголовном судопроизводстве следователи используют стандартные формы для документирования своего анализа, а также следят за тем, чтобы они не забыли выполнить все этапы расследования, чтобы получить исчерпывающее исследование потерпевшего и компьютерная система подозреваемого. Аналогичным образом следует вести записи, описывающие все этапы работы с доказательствами, будь то место преступления или судебно-медицинская лаборатория. Снимки экрана, фотографии и видеозаписи значительно повышают качество контрольного следа электронных доказательств.

Поддержка специалистов: во многих случаях высокотехнологичный характер компьютерной среды и содержащихся в ней данных требует использования специалистов по компьютерной криминалистике. Потребность в поддержке специалистов может быть вызвана узкоспециализированной областью цифровой криминалистики (например, анализ мобильных вредоносных программ), а также ограниченной доступностью оборудования для такого анализа. Следовательно, хотя и не обязательно в обязательном порядке во всех случаях, специализированный анализ будет важной частью материалов дела, что еще больше усилит аргументы стороны, желающей представить такие доказательства.

Законность: Компьютерные системы, которые используются в качестве источника электронных доказательств, обычно содержат по крайней мере некоторый объем частной информации, которая не будет иметь отношения к расследованию или иметь ценность для расследования. Следовательно, необходима надлежащая сортировка данных, имеющих отношение к расследованию, и конфиденциальной информации, которую нельзя изучать. В некоторых случаях эти различия не будут четко проводиться; таким образом, судебные постановления о сохранении таких данных могут потребоваться для дальнейшего анализа информации.

Список использованных источников

1. UNODC - Basic Manual on the Detection And Investigation of the Laundering of Crime Proceeds Using Virtual Currencies

ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ И ПРОИЗВОДСТВЕ

Рязанова Анна Максимовна, курсант, рядовой полиции
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Развитие космических информационных технологий

В 2021 году празднуется 60-летняя годовщина полета Ю.А. Гагарина в космос. И последние полвека космос является одним из ведущих отраслей народного хозяйства. И актуальной темой на данный момент являются именно информационно-технические космические технологии.

Три десятилетия космической эры существенно повлияли на наши знания о Земле, на технологию создания карт, на оперативные наблюдения за природными процессами, особенно в метеорологии.

При помощи искусственных спутников оказалось возможным предсказывать на 3-5-дневный срок погоду на большей части Земли с точностью и покрытием, ранее недоступными; наблюдать явления засухи в крупных регионах; выявлять лесные пожары и сведение лесов в малообжитых районах; выявлять биопродуктивные зоны океана, наиболее подходящие для обитания рыб; определять смещения тектонических плит и прогнозировать землетрясения по параметрам траекторий орбит ИСЗ.

Космические методы приобретают решающую роль в решении современной проблемы человечества - изучении Земли как планеты. Эффективность практического использования космических методов будет в значительной степени определяться развитием разветвленной сети геоинформационных систем, которые должны обеспечить широкий доступ к космическим данным.

Космические технологии развиваются всё больше и видны огромные перспективы их развитий.

1.Использование космических технологий для борьбы с вирусами

Российские космические технологии намерена использовать французская компания "Эр ин спейс" для защиты иммунодефицитных больных и для борьбы с вирусом птичьего гриппа.

Внимание французских медицинских специалистов привлекли российские методики плазменной очистки воздуха от биологического загрязнения на космических станциях. Они были разработаны еще в 90-е годы минувшего века и с успехом использовались на орбитальном комплексе "Мир". С апреля 2001 года такие устройства применяются и для очистки воздуха в российском сегменте.

Международной космической станции. Французская компания "Эр ин спейс" адаптировала их к наземным госпитальным условиям с помощью Европейского космического агентства, осуществляющего масштабную программу передачи космических технологий. Сертификация оборудования проводилась в Лаборатории вирусологии в Лионе. По словам специалистов российское изобретение позволяет, в частности, полностью уничтожать в воздухе вирусы птичьего гриппа даже при сильной их концентрации.

По мнению французских экспертов, в случае пандемии птичьего гриппа такие технологии можно быстро переоборудовать в больницы, например, школьные помещения. Разработка также может быть успешно использована для стерилизации операционных и лабораторных помещений, подчеркивают специалисты.

2.Космические технологии будущего

Магнитный космический поезд Startram

Проект предложенной системы космических запусков Startram, для старта строительства и реализации которого потребуется, по предварительным меркам, около 20

миллиардов долларов, обещает возможность доставки на орбиту грузов весом до 300 000 тонн с очень демократичной ценой в 40 долларов за килограмм полезной нагрузки. Если учесть, что в настоящий момент стоимость доставки 1 кг полезной нагрузки в космос составляет в лучшем случае 11 000 долларов, проект выглядит весьма интересным.

Для реализации проекта Startram не потребуются ракеты, топливо или ионные двигатели. Вместо всего этого здесь будет использоваться технология магнитного отталкивания. Стоит отметить, что концепт поезда на магнитной подушке далеко не нов. На Земле уже функционируют составы, которые двигаются по магнитному полотну со скоростью около 600 километров в час. Однако на пути всех этих маглевов (использующихся преимущественно в Японии) находится одно серьезное препятствие, которое ограничивает их максимальную скорость. Для того чтобы такие поезда смогли раскрыть свой полный потенциал и достигать максимально возможной скорости, нам необходимо избавиться от атмосферного воздействия, которое замедляет их движение.

Проект Startram предлагает решение этого вопроса путем строительства длинного навесного вакуумного тоннеля на высоте около 20 километров. На такой высоте сопротивление воздуха становится менее выраженным, что позволит производить космические запуски на гораздо более высоких скоростях и с гораздо меньшим сопротивлением. Космические аппараты в буквальном смысле будут выстреливаться в космос, без необходимости в преодолении атмосферы. Строительство такой системы потребует около 20 лет работы и инвестиций на общую сумму в 60 миллиардов долларов.

3. Солнечный зонд

Как и на Земле, на Солнце тоже есть свои ветра и шторма. Однако в отличие от земных, солнечные ветра очень опасны для человека.. На многие вопросы о Солнце, ответов на которые нет до сих пор, по мнению аэрокосмического агентства NASA, сможет ответить «Солнечный зонд», который отправился к нашему светилу в 2018 году.

Космический аппарат должен будет приблизится к Солнцу на расстояние около 6 миллионов километров. Это приведет к тому, что зонду придется испытать на себе воздействие радиационной энергии такой мощности, какую не испытывал ни один рукотворный космический аппарат. Защититься от воздействия губительной радиации зонду, по мнению инженеров и ученых, поможет карбоно-композитный тепловой экран толщиной 12 сантиметров.

Однако NASA не может просто направить зонд сразу к Солнцу. Космическому аппарату придется сделать как минимум семь орбитальных пролетов вокруг Венеры. А на это у него уйдет около семи лет. Каждый оборот будет ускорять зонд и подстраивать траекторию для правильного курса. После последнего облета зонд направится к орбите Солнца, на расстояние 5,8 миллиона километров от его поверхности. Таким образом он станет наиболее приближенным к Солнцу рукотворным космическим объектом. Нынешний рекорд принадлежит космическому зонду «Гелиос-2», который находится на расстоянии примерно 43,5 миллиона километров от Солнца.

4. 3D-напечатанные марсианские дома

Чтобы приблизить момент начала подготовки полета человека на Марс, NASA организовало архитектурный конкурс, задачей которого является разработка и спонсирование технологий 3D-печати, которые позволят методом трехмерной печати строить марсианские дома.

Единственное условие конкурса заключалось в использовании материалов, которые широко доступны для добычи на Марсе. Победителями стали две дизайнерские компании из Нью-Йорка, TeamSpaceExplorationArchitecture и CloudsArchitectureOffice, предложившие свой концепт марсианского дома ICE HOUSE. В качестве основы концепт предлагает использование льда (отсюда и название). Строительство зданий будет производиться в ледяных зонах Марса, куда будут отправляться посадочные модули, загруженные множеством компактных роботов, которые будут собирать грязь и лед для возведения сооружений вокруг этих модулей.

Стенки сооружений будут выполнены из смеси воды, геля и кремнезема. Как только материал замерзнет благодаря низким температурам на поверхности Марса, получится весьма себе подходящее для жилища помещение с двойными стенками. Первая стенка будет состоять из ледяной смеси и предоставлять дополнительную защиту от радиации, роль второй стенки будет выполнять сам модуль.

Освоение космоса не только стимулировало интерес к образованию, но и позволило использовать великолепные технические средства - радиовещательные и телевизионные спутники для образовательных целей. Широкие массы населения планеты могут получить через всеобщую глобальную систему образования, построенного на использовании мировых космических систем связи и телевидения на основе использованных спутников Земли, самые обширные знания. Радио - и телепередачи через спутники позволят решать проблемы ликвидации неграмотности, повышать образовательный ценз детей и взрослых и т.п. Таким образом, космос и образование оказались элементами двуединого процесса: без глубоких знаний невозможно покорение космоса, последнее же в свою очередь, дает эффективное средство для всестороннего совершенствования и развития образования.

Космонавтика нужна науке - она грандиозный и могучий инструмент изучения Вселенной, Земли, самого человека. С каждым днем все более расширяется сфера прикладного использования космонавтики. Служба погоды, навигация, спасение людей и спасение лесов, всемирное телевидение, всеобъемлющая связь, сверхчистые лекарства и полупроводники с орбиты, самая передовая технология - это уже и сегодняшний день, и очень близкий завтрашний день космонавтики. А впереди - электростанции в космосе, удаление вредных производств с поверхности планеты, заводы на околоземной орбите и Луне, и т.д.

Космическое будущее человечества - залог его непрерывного развития на пути прогресса и процветания, о котором мечтали и которое создают те, кто работал и работает сегодня в области космонавтики и других отраслях народного хозяйства.

Список использованных источников

1. "Космическая техника" / под ред. К. Гэтланда, М.: Мир, 1986

2. "Космические методы изучения биосферы"/ ответств. ред. Л.Н. Васильев, М.: Наука, 1990

3. Освоение космического пространства в СССР (по материалам печати) / ответств. ред. Р.З. Сагдеев, М.: Наука, 1987

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В СИСТЕМЕ ОБРАЗОВАНИЯ

Рязанов Максим Игоревич, курсант 2-ого курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

В настоящее время в сфере образования существует ряд понятий, связанных с интенсивным процессом информатизации.

Информационные технологии – это совокупность знаний о способах и средствах работы с информационными ресурсами, и способ сбора, обработки и передачи информации для получения новых сведений об изучаемом объекте.

Информационная технология – это педагогическая технология, использующая специальные способы, программные и технические средства (кино, аудио – и видео средства, компьютеры) для работы с информацией.

Компьютерные технологии – это вспомогательные средства в процессе обучения, так как передача информации – это не передача знаний.

Последние годы термин «информационные технологии» часто выступает синонимом термина «компьютерные технологии», так как все информационные технологии в настоящее время так или иначе связаны с применением компьютера. Однако, термин «информационные технологии» намного шире и включает в себя «компьютерные технологии» в качестве составляющей. При этом информационные технологии, основанные на использование современных компьютерных и сетевых средств, образуют термин «Современные информационные технологии».

Информационные и коммуникационные технологии (ИКТ) – это обобщающее понятие, описывающее различные устройства, механизмы, способы, алгоритмы обработки информации. Важнейшим современным устройствами ИКТ являются компьютер, снабженный соответствующим программным обеспечением и средства телекоммуникаций вместе с размещенной на них информацией.

Под средствами современных информационных и коммуникационных технологий понимают программные, программно-аппаратные и технические средства, а так же устройства, функционирующие на базе микропроцессорной, вычислительной техники, а также современных средств и систем транслирования информации, информационного обмена, обеспечивающие операции по сбору, продуцированию, накоплению, хранению, обработке, передаче информации и возможность доступа к информационным ресурсам компьютерных сетей (в том числе глобальных) .

К средствам современных информационных и коммуникационных технологий относятся ЭВМ, ПЭВМ, комплекты терминального оборудования для ЭВМ всех классов, локальные вычислительные сети, устройства ввода,

вывода информации, средства ввода и манипулирования текстовой и графической информацией, средства архивного хранения больших объемов информации и другое периферийное оборудование современных ЭВМ; устройства для преобразования данных из графической или звуковой формы представления данных в цифровую и обратно; средства и устройства манипулирования аудиовизуальной информацией (на базе технологий Мультимедиа и «Виртуальная реальность») ; системы искусственного интеллекта; системы машинной графики, программные комплексы (языки программирования, трансляторы, компиляторы, операционные системы, пакеты прикладных программ и пр.) и др.; современные средства связи, обеспечивающие информационное взаимодействие пользователей как на локальном уровне (например, в рамках одной организации или нескольких организаций), так и глобальном (в рамках всемирной информационной среды).

Основными направлениями применения информационных технологий в учебном процессе являются:

- разработка педагогических программных средств различного назначения;
- разработка web-сайтов учебного назначения;
- разработка методических и дидактических материалов;
- осуществление поиска информации различных форм в глобальных и локальных сетях, её сбора, накопления, хранения, обработки и передачи;
- создание электронных библиотек;
- организация интеллектуального досуга учащихся.

Современные технологии и телекоммуникации позволяют изменить характер организации учебно-воспитательного процесса, полностью погрузить обучаемого в информационно-образовательную среду, повысить качество образования, мотивировать процессы восприятия информации и получения знаний. Новые информационные технологии создают среду компьютерной и телекоммуникационной поддержки организации и управления в различных сферах деятельности, в том числе и в образовании. Осуществляемая в стране реформация школы направлена на то, чтобы привести содержание образования в соответствие с современным уровнем научного знания, повысить эффективность всей учебно-воспитательной работы и подготовить учащихся к деятельности в условиях перехода к информационному обществу. Поэтому информационные технологии становятся неотъемлемым компонентом содержания обучения, средством оптимизации и повышения эффективности учебного процесса, а также способствуют реализации многих принципов развивающего обучения.

Практически во всех развитых странах сделан резкий поворот на обучение умению самостоятельно добывать нужную информацию, вычленять проблемы и искать пути их рационального решения, уметь критически анализировать получаемые знания и применять их для решения новых задач. Идеальная система обучения должна:

- Сформировать у обучающегося желание учиться и цель обучения.
- Обеспечить каждого учащегося индивидуально-адаптированными учебными пособиями.
- Поддерживать мотивацию к обучению и творческой деятельности.
- Дать каждому учащемуся возможность занятий по индивидуальному графику.
- Непрерывно оценивать результаты обучения.
- Педагог может предложить обучаемым универсальные программные продукты (например, изучаемые в школе и вузе графические и текстовые редакторы, электронные таблицы и т.п.).

Текстовые редакторы стимулируют работу по выполнению различных письменных заданий: сочинений, эссе, рефератов и др. Они облегчают как их первоначальное оформление, так и последующие изменения, и дополнения. Работа с такой программой, с одной стороны, прививает обучаемым чисто технические навыки электронного набора и оформления текста. С другой — это мощный инструмент, мотивирующий обучаемых к совершенствованию первоначальных результатов. Если же работа выполняется на компьютере, включенном в сеть, то появляется также возможность совместной работы обучаемых и педагога — внесение последним своих замечаний непосредственно в текст по ходу его создания.

Электронные таблицы. Программы, относящиеся к этой категории (например, Microsoft Excel), дают возможность без изучения языков программирования выполнять расчеты по сложным формулам, включающим в себя проверку различных условий и реализующим циклические алгоритмы и ветвления (например, найти сумму или количество чисел, удовлетворяющих некоторому условию). Результаты вычислений обновляются автоматически при изменении входящих в формулу параметров. По данным таблиц можно построить график или диаграмму, один только выбор которых может стать самостоятельным заданием. Диаграммы и графики не являются статичными — каждый раз при изменении использующихся при их построении данных они меняют свою конфигурацию. Все

перечисленные особенности делают электронные таблицы прекрасным инструментом для компьютерного моделирования. Обучаемым не требуется писать специальную компьютерную программу. Достаточно внести в таблицу формулы, отражающие суть математической модели, а затем, изменяя исходные данные, наблюдать их влияние на графиках.

Графические редакторы позволяют ему легко строить сложные геометрические объекты, изучать их преобразования (растяжение, сжатие, сдвиг, поворот, отображение), строить произвольные проекции. Все это способствует развитию у обучаемых пространственного воображения. Наиболее широко в данный момент используются интегрированные уроки с применением мультимедийных средств. Обучающие презентации становятся неотъемлемой частью обучения, но это лишь простейший пример применения информационных технологий.

Инструментальные средства для обеспечения коммуникаций.

Новый импульс информатизации образования дает развитие информационных телекоммуникационных сетей. Глобальная сеть Internet обеспечивает доступ к гигантским объемам информации, хранящимся в различных уголках нашей планеты. Многие эксперты рассматривают технологии Internet как революционный прорыв, превосходящий по своей значимости появление персонального компьютера.

Инструментальные средства компьютерных коммуникаций включают несколько форм: электронную почту, электронную конференция связь, видеоконференцсвязь, Internet. Эти средства позволяют преподавателям и обучаемым совместно использовать информацию, сотрудничать в решении общих проблем, публиковать свои идеи или комментарии, участвовать в решении задач и их обсуждении

Электронная почта (e-mail) — это асинхронная коммуникационная среда, что означает: для получения сообщения не требуется согласовывать время и место получения с отправителем, и наоборот. Электронная почта может использоваться как для связи между двумя абонентами, так и для соединения одного — многих получателей. Эти особенности ее работы целесообразно использовать для установления обратной связи между преподавателями или обучающими программами и одним или несколькими обучаемыми независимо от их физического расположения. Электронная почта широко применяется также для координации и установления обратной связи в дистанционном и открытом обучении.

Необходимо заметить, что образовательные возможности электронной почты наиболее доступны из всех информационных и телекоммуникационных технологий. Специальные почтовые программы основаны на сходных принципах, и, соответственно, для пользования электронной почтой не требуется серьезной профессиональной подготовки. Электронная почта имеет очень широкие возможности для улучшения качества образовательного процесса. Это и средство дополнительной поддержки учебно-познавательной деятельности, дающее прекрасные возможности общения обучаемых с преподавателем и друг с другом (причем — конфиденциального общения), и средство управления ходом образовательного процесса.

Электронная конференцсвязь — асинхронная коммуникационная среда, которая подобно электронной почте может использоваться для плодотворного сотрудничества обучаемых и педагогов, являясь пользователям неким структурированным форумом, на котором можно в письменном виде изложить свое мнение, задать вопрос и прочитать реплики других участников. Участие в тематических электронных конференциях сети Internet очень плодотворно для самообразования педагогов и обучаемых. Электронные конференции могут быть организованы и в пределах локальной сети отдельного учебного заведения для проведения семинаров, протяженных по времени дискуссий и т.п. Асинхронный режим работы обучаемого способствует рефлексии и, соответственно, продуманности вопросов и ответов, а возможности использования файлов любого типа (графика, звук, анимации) делают такие виртуальные семинары весьма эффективными.

Видеоконференцсвязь — в отличие от предыдущей формы имеет синхронный характер, когда участники взаимодействуют в реальном времени. Здесь возможно общение типа один на один (консультация), один ко многим (лекция), многие ко многим (телемост).

Эта коммуникационная технология в настоящее время используется преимущественно в высших учебных заведениях, имеющих разветвленную сеть филиалов. Основное препятствие для широкого использования — дорогое оборудование, которое не всегда доступно в локальных учебных центрах (филиалах) головного учебного заведения.

WWW технология. Компьютерные коммуникации выступают также как средство доступа к такой технологии Internet, как WWW (Word Wide Web), или Всемирной Паутине, состоящей из сотен миллионов информационных сайтов, связанных гиперссылками. С точки зрения образовательных возможностей это отнюдь не пассивный ресурс, а среда, стимулирующая активность и самостоятельность обучаемых. В ней можно заниматься поиском информации, но результаты зачастую непредсказуемы и зависят от находчивости и инициативности пользователя. WWW позволяет вступать в контакт с другими людьми (в синхронном или асинхронном режиме) или интерактивными программами, отвечая на вопросы или заполняя специальные формы на Web-страницах. Наконец, можно стать одним из миллионов «строителей» Всемирной Паутины, создавая Web-страницы и размещая их в WWW.

К числу базовых обычно относят следующие технологии Internet: WWW(англ. World Wide Web — Всемирная Паутина) — технология работы в сети с гипертекстами;

- FTP (англ. File Transfer Protocol — протокол передачи файлов) — технология передачи по сети файлов произвольного формата;
- IRC (англ. Internet Relay Chat — поочередный разговор в сети, чат) — технология ведения переговоров в реальном масштабе времени, дающая возможность разговаривать с другими людьми по сети в режиме прямого диалога;
- ICQ (англ. I seek you — я ищу тебя, можно записать тремя указанными буквами) — технология ведения переговоров один на один в синхронном режиме.

Специфика технологий Internet заключается в том, что они предоставляют и обучаемым, и педагогам громадные возможности выбора источников информации, необходимой в образовательном процессе:

- базовая информация, размещенная на Web и FTP-серверах сети;
- оперативная информация, систематически пересылаемая заказчику по электронной почте в соответствии с выбранным списком рассылки;
- разнообразные базы данных ведущих библиотек, информационных, научных и учебных центров, музеев;
- информация о компакт-дисках, видео и аудиокассетах, книгах и журналах, распространяемых через Internet-магазины.

МОДЕРНИЗАЦИЯ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УПРАВЛЕНИЯ УРОВНЯ ВОДЫ В БАРАБАНЕ КОТЛА-УТИЛИЗАТОРА ЗА ПЕЧЬЮ ОТЖИГА В СПЦ-1 АО «ОЭМК ИМ. А.А УГАРОВА»

Сабынин Андрей Михайлович, студент 4-го курса
Научный руководитель Хархота Надежда Васильевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) ФГАОУ ВО «Национальный исследовательский технологический институт «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Важнейшая роль принадлежит теплотехническим процессам в производстве и термической обработке проката. Не менее важным этапом в производстве служит отвод горячих паров и газов от печей отжига.

Котёл-утилизатор (КУ) – котёл, использующий (утилизирующий) теплоту отходящих газов различных технологических установок.

Применение котлов утилизаторов существенно повышает эффективность работы оборудования, результатом работы которого являются выхлопные газы или пар. [2]

Целью исследования является анализ автоматической системы регулирования уровня воды в барабане котла-утилизатора за печью отжига в СПЦ-1 АО «ОЭМК им. А.А. Угарова».

Задачи исследования:

- изучить характеристику технологического процесса;
- проанализировать существующий уровень автоматизации;
- выявить недостатки существующей системы управления и определить задачи для модернизации системы управления.

Объектом исследования является котел-утилизатор за печью отжига в СПЦ-1 АО «ОЭМК им. А.А. Угарова».

Предмет исследования автоматизированная система управления уровнем воды в барабане котла утилизатора за печью отжига СПЦ-1 АО «ОЭМК им А.А Угарова»

Для утилизации тепла, охлаждения дымовых газов и выработки насыщенного пара давлением 10 кгс/см^2 за печами отжига СПЦ-1 установлены три котла-утилизатора типа Г-1030Б.

Котёл-утилизатор типа Г-1030Б горизонтальный, газотрубного типа, двух барабанный, с естественной циркуляцией, установлен на обводной линии основного дымопровода “печь-дымосос-дымовая труба” на бетонном фундаменте отметка - 5.200 м, на двух подвижных и одной неподвижной опорах. Он состоит из блока котла, входной газовой камеры и выходной газовой камеры. Для ведения и регулирования процессов эксплуатации котёл-утилизатор оборудован: отсекающими шиберами по дымовому тракту, трубопроводами и запорной арматурой, системой автоматического контроля и регулирования, вспомогательным оборудованием. [1]

Для осуществления регулирования режима работы котла-утилизатора и контроля за параметрами его работы, на групповом щите контроля КИПиА и на щите контроля КИПиА котла установлены следующие приборы автоматического контроля, которые определяют следующие параметры:

- температура питательной воды перед котлом-утилизатором;
- давление питательной воды к котлу-утилизатору;
- температура дымовых газов перед котлом-утилизатором;
- температура дымовых газов после котла-утилизатора;
- давление пара в паропроводе;
- давление пара в барабане-паросборнике;
- расход пара от котла-утилизатора;
- уровень воды в барабане-паросборнике;
- температура пара от котла-утилизатора.

На котле-утилизаторе имеются системы автоматического регулирования уровня воды в барабане-паросборнике, а также температуры и уровня воды в колодце-охладителе. Автоматическое регулирование уровня воды в барабане-паросборнике осуществляется трёхимпульсным регулятором, который воздействует на регулирующий клапан на узле питания котла-утилизатора. Импульсами для регулирования служат: уровень воды в барабане-паросборнике, расход питательной воды на котел-утилизатор и расход пара от котла-утилизатора.

Особенности технологического процесса, в котором участвуют котлы утилизаторы, накладывают определённые требования на задачу управления ими. Главной из особенностей, отличающих КУ от обычных промышленных котлов является то, что ведущим регулирующим параметром является не выработка пара, которая определяет расход необходимой энергии топлива, а количество энергии, вносимой потоком отходящих технологических газов и определяющей выработку пара, как реакцию КУ на режим тепловой работы, задаваемый технологическим агрегатом. [4]

В обычных топочных котлах управляя расходом топлива и воздуха добиваются получения таких объёмов и температур газов в конце топки, которые позволяют образовать пар необходимого качества и в необходимом количестве. В КУ наоборот расход и температура газа заданы.

Количество же пара соответствует энергии, отданной рабочему теплу (воде) отходящими от теплотехнических агрегатов газами. Таким образом, управление КУ состоит в том, чтобы обеспечить надёжную утилизацию теплоты отходящих газов технологической установки путём образования соответствующего количества пара заданных параметров (давления и температуры пара). [3]

К недостаткам систем автоматизации относится:

- отсутствие автоматического регулирования разряжения внутри котла утилизатора, что приводит к нестабильной работе, частым остановкам и запускам котла;
- система предусматривает только световую и звуковую аварийную сигнализацию и не имеет автоматической аварийной защиты;
- морально и физически устаревшие средства автоматизации.

Для модернизации АСУ предлагается:

1.Разработать современную и надежную систему автоматического регулирования уровня воды в барабане котла-утилизатора с учетом действующих возмущений, которая позволит вырабатывать необходимое количество пара.

2. Так как производить управление режимами работы дымососа в конце общего дымохода мы не имеем возможности, является целесообразным произвести автоматизацию шиберов на входе и выходе КУ, что позволит создавать необходимое разряжение, а также снизить количество остановок и пусков КУ, как следствие увеличится количество производимого пара.

3. Произвести замену физически и морально устаревших датчиков, а так же произвести выбор современного программно-логического контроллера.

4. Разработать систему визуализации технологического процесса.

В процессе исследования была разработана математическая модель контур регулирования уровня воды в барабане котла, рисунок 1. Математическая модель является методом научного исследования, который основан на познании изучаемых процессов с помощью математической модели. От регулятора идёт управляющее воздействие на исполнительный механизм через преобразователь представляющий собой трёхпозиционный релейный элемент. Исполнительным механизмом является задвижка с электроприводом, моделью которого является идеальное интегрирующее звено с коэффициентом K_1. Объект управления – барабан КУ.

Коэффициент K_1 характеризует изменение расхода воды в зависимости от положения заслонки:

$$K_1 = \frac{Q_{max}}{T}\ , \qquad (1)$$

где Qmax – максимальная пропускная способность трубопровода, кг/сек;

T - время полного хода выходного вала, сек.

Объектом управления является барабан котла, в котором изменение расхода воды вызывает изменение уровня – интегрирующее звено. Коэффициент K определяется по формуле:

$$K_2 = \frac{1}{S}\ , \qquad (2)$$

где S – площадь резервуара (барабана), м^2.

Так же для решения поставленных задач необходимо:

- выбрать исполнительный механизм Sipos Ecotron 5 фирмы Siemens;
- электромагнитный расходомер «Взлет ЭРСВ-440»;
- датчик давления «Метран-150-ДД»;
- вихревой расходомер «ЭМИС-ВИХРЬ 200»;
- датчик давления «Метран» 150-ДИ;
- контроллер SIMATIC S7-1500.

Замена оборудования на оборудование из этого списка позволит добиться экономии ресурсов производства и повышении надежности системы управлении а также более информативное, точное, безопасное оборудование придет на замену морально устаревшему.

Список использованных источников

1. Бородин И.Ф. Автоматизация технологических процессов и системы автоматического управления: учебник для СПО/ И.Ф. Бородин, С.А. Андреев. - 2 -е изд., испр. и доп.. - М.: Издательство Юрайт, 2019. -386с.

2. Иванов А. А. Автоматизация технологических процессов и производств : учебное пособие / А.А. Иванов. - 2-е изд., испр. и доп. - М. : ФОРУМ, ИНФРА-М, 2018. - 224 с.

3. Молоканова Н. П. Автоматическое управление. Курс лекций с решением задач и лабораторных работ: учебное пособие / Н.П. Молоканова. - М. : ФОРУМ, 2017. - 224 с.

4. Схиртладзе А. Г. Автоматизация технологических процессов и производств : учебник / А. Г. Схиртладзе, А. В. Федотов, В. Г. Хомченко. — 2-е изд. — Саратов : Ай Пи Эр Медиа, 2019. — 459 с. — ISBN 978-5-4486-0574-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/83341.html. — Режим доступа: для авторизир. Пользователей.

НЕГАТИВНОЕ ВЛИЯНИЕ ТИК ТОКА НА МОРАЛЬНО-ПСИХОЛОГИЧЕСКОЕ РАЗВИТИЕ НЕСОВЕРШЕННОЛЕТНИХ

Савгачев Михаил Владиславович, курсант 4-го курса
Научный руководитель Овчинский Анатолий Семёнович, доктора технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

ТикТок - популярный во всем мире сервис для создания и просмотра коротких видеороликов. В тик токе основном циркулирует развлекательный контент,и даже встречаются научные и познавательные видеоролики. В связи с ростом популярности данного сервиса, он стал привлекательным для лиц, преследующих корыстные цели и других сомнительных личностей.

Основной контингент тиктока это дети в возрасте от 13 до 15 лет.

Контент оказывающий деструктивное воздействие на психику несовершеннолетних можно условно разделить на несколько категорий:

1) Контент поддерживающий неформальные сообщества. Здесь ключевую роль играет юношеский максимализм, стремление выделиться из толпы и быть не таким как все. Под этим предлогом несовершеннолетние относят себя к различным неформальнымм группам, таким как ЛГБТ-сообщество, различным гендерам (здесь стоит отметить, что помимо мужчины и женщины были придуманы ещё порядка 10 различных гендеров). Примером может послужить известный тикток блогер - Оля Тыква, имеющий на своём аккаунте 1 млн подписчиков. Девочка родилась в 2006 году, то есть на данный момент девушке всего 15 лет. Девушка открыто выступает в поддержку ЛГБТ-сообщества. Ролики данной девушки собирают немалое количество просмотров, а также находят поддержку среди своих ровесников.(Здесь 2 видеоролика)

2) Непредсказуемые челленджи. Челлендж - жанр видеороликов, в котором блогер выполняет задание и предлагает повторить это задание другим пользователям, зафиксировав попытку на видео. Примером опасного челленджа служит задание с хэштэгом Pass Out Challange - суть которого заключается в том, чтобы в положении сидя задержать дыхание, а потом резко встать на ноги, результатом чего будет потеря сознания. Выполняя такое действие человек, лишает мозг кислорода, наступает обморок. С мозгом происходит всё то же самое, что и во время удушья или остановки сердца. Начинается гипоксия мозга, падение уровня кислорода в мозге может вызвать смерть. Но несовершеннолетние пользователи в силу своей необразованности, а также стремлению подражать своему кумиру и быть в трене не осознают опасность данного действия.(Видео)

3) Контент сексуального характера. Здесь несовершеннолетние пользователи выкладывают видеоролики о своих достижениях в половой жизни, и призывают своих подписчиков, таких же несовершеннолетних вступать в половые связи.

4) Черный юмор. Ролики данного типа оказывают негативное влияние на развитие моральной составляющей несовершеннолетних. В таких видеороликах высмеиваются люди с ограниченными возможностями, погибшие животные и погибшие люди.

5) Видеоролики, преследующие определённые цели (к примеру смена политического режима). Это достаточно актуальная тема в России в связи с последними событиями. Опять же, отсутствие должного развития и способности анализировать информацию несовершеннолетние как губка впитывают всё, что им преподносят на данном ресурсе. Мотивами выйти на акции протестов выступают идеи свободной России, смена политического режима, борьба с коррупцией. Но всё это делается с целью дискредитации правительства путём (введения в зублуждение) от якобы принятых антинародных законов законов(видео).

Также видеоблогеры дисркдитируют полицейских и правоохранительную систему России следующими видеороликами(видеоролик)

В заключении хочу сказать, что изначально митинг планировались как мирный протест, но на нём оказались граждане, которые применяли физическую силу в отношении полициейских. И ролики где применяют физическую силу в отношении полицейских, неразумные граждане высказывают слова поддержки атакующим.

Секция 2.3

ВЫЯВЛЕНИЕ КАНАЛОВ УТЕЧКИ И НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ

Абдульманова Амина Олеговна, курсант1-го курса МосУ МВД России имени В.Я Кикотя

Научный руководитель Овчинский Анатолий Семёнович профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

В настоящее время необходимость в защите информации, содержащейся в информационных системах правоохранительных органов, не вызывает сомнений. Сущность защитных мероприятий сводится к перекрытию возможных каналов утечки защищаемой информации, которые появляются в силу объективно складывающихся условий ее распространения и возникающей у конкурентов заинтересованности в ее получении. Каналы утечки информации достаточно многочисленны. Они могут быть как естественными, так и искусственными, т. е. созданными с помощью технических средств. Рассмотрим возможные каналы утечки информации и несанкционированного доступа к ресурсам, которые могут быть использованы противником в данном помещении, а также возможную защиту от них.

Основные причины утечки информации:

- Случайная утечка информации через сеть интернет или ошибки сотрудников. Персонал может даже не знать о существовании конфиденциальной информации и своими действиями случайно привести к ее утечке.
- Использование неисправных или нелицензионных технических средств для обработки важной информации.
- Большая текучка кадров. Работники, которых уволили, могут распространять конфиденциальную информацию компании.
- Неблагоприятные погодные условия, стихийное бедствие, техногенные аварии и катастрофы также могут стать причиной утечки информации.
- Ведение конкурентами технической или агентурной разведки.

В соответствии с ГОСТ Р 50922—96 рассматриваются три вида утечки информации:

- разглашение;
- несанкционированный доступ к информации;
- получение защищаемой информации разведками (как отечественными, так и иностранными).

Организационно-технические мероприятия обеспечивают блокирование разглашения и утечки конфиденциальных сведений через технические средства обеспечения производственной и трудовой деятельности, а также противодействие техническим средствам промышленного шпионажа с помощью специальных технических средств, устанавливаемых на элементы конструкций зданий, помещений и технических средств, потенциально образующих каналы утечки информации.

В этих целях возможно использование:

- технических средств пассивной защиты, например фильтров, ограничителей и тому подобных средств развязки акустических, электрических и электромагнитных систем защиты сетей телефонной связи, энергоснабжения, радиофикации и др.;
- технических средств активной защиты: датчиков акустических шумов и электромагнитных помех.

Список использованных источников

1. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. — Рн/Д: Феникс, 2017. — 324 с.

ВЛИЯНИЕ КИБЕРВОЙНЫ НА ЛЮДЕЙ

Авдеев Даниил Викторович студент 1-ого курса
Научный руководитель Овчинский Анатолий Семёнович профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

При кибервойне страны агрессоры будут выкачивать информацию из любого найденного или созданного канала утечки, могут выкачивать у обычных граждан или на военных базах, в зависимости от того что они будут использовать для достижения своих целей, так же могут взламываться сервера, без которых будет ограничен вход в интернет и получается, что нарушаются личные права человека, если конечно страна с демократической формой правления.

Это военные действия, осуществляемые не физически, а электронно, когда в качестве оружия выступает информация, а инструментами являются компьютеры и интернет. Кибервойна, таким образом, является одним из видов информационной войны, задача которой — достичь определенных целей в экономической, политической, военной и других областях посредством воздействия на общество и власть тщательно подготовленной информацией.

Хотя войну нового времени можно назвать психологической, противостояние в кибернетическом пространстве представляет реальную опасность. Компьютерные технологии и Интернет получили широкое распространение по всему миру и используются не только в повседневной жизни граждан, но и на предприятиях, в государственных учреждениях, которые в свою очередь являются важной структурной единицей страны. Вредоносное воздействие на инфраструктуру, заводы, больницы представляет угрозу для национальной безопасности стран.

Угрозы информационной безопасности – кибервойны. Кибервойны — это военные действия, осуществляемые не физически, а электронно, когда в качестве оружия выступает информация, а инструментами являются компьютеры и интернет. Кибервойна, таким образом, является одним из видов информационной войны, задача которой — достичь определенных целей в экономической, политической, военной и других областях посредством воздействия на общество и власть тщательно подготовленной информацией. Хотя войну нового времени можно назвать психологической, противостояние в кибернетическом пространстве представляет реальную опасность. Компьютерные технологии и Интернет получили широкое распространение по всему миру и используются не только в повседневной жизни граждан, но и на предприятиях, в государственных учреждениях, которые в свою очередь являются важной структурной единицей страны. Вредоносное воздействие на инфраструктуру, заводы, больницы представляет угрозу для национальной безопасности стран. Высоким приоритетом кибервойны является не только нанесение ущерба противнику, но и защита собственных данных, поэтому кибербезопасность — неотъемлемая часть подобного рода противостояний. Она представляет собой совокупность принципов, средств и стратегий для обеспечения неуязвимости и защиты киберсреды, доступности, целостности и конфиденциальности данных. Способы и этапы ведения кибервойны Кибернетическая война состоит из двух

этапов: шпионаж и атаки. Первый этап подразумевает сбор данных посредством взлома компьютерных систем других государств. Атаки можно разделить на типы в зависимости от цели и задач военных действий: Вандализм — размещение пропагандистских или оскорбительных картинок на веб-страницах вместо исходной информации. Пропаганда и информационная война — использование пропаганды в контенте веб-страниц, в почтовых и других подобных рассылках. Утечки конфиденциальных данных — все, что представляет интерес, копируется со взломанных частных страниц и серверов, также секретные данные могут быть подменены. DDoS-атаки — поток запросов со множества машин с целью нарушить функционирование сайта,
системы компьютерных устройств. Нарушение работы компьютерной техники — атаке подвергаются компьютеры, отвечающие за функционирование оборудования военного или гражданского назначения. Нападение приводит к выходу техники из строя или к ее отключению. Атаки на инфраструктурные и критически важные объекты и кибертерроризм — воздействие на машины, которые регулируют инженерные, телекоммуникационные, транспортные и другие системы, обеспечивающие жизнедеятельность населения.

Цели кибервойны все операции кибервойны направлены на нарушение функционирования вычислительных систем, отвечающих за работу деловых и финансовых центров, государственных организаций, на создание беспорядка в жизни страны, поэтому в первую очередь страдают важные жизнеобеспечивающие и функциональные системы населенных пунктов. К ним относятся системы водоснабжения, канализация, электростанции, энергетические узлы, другие коммуникационные сети.

Источник угрозы зависимость госучреждений, предприятий и простых граждан от интернета значительно возросла. Соответственно, кибератаки одного государства, направленные против другого, могут нанести весомый ущерб экономике страны, так что кибервойна является реальной угрозой. При этом создание компьютерного вируса или «троянского коня» обойдется значительно дешевле, чем разработка и покупка оружия и ракет, а урон, нанесенный кибервторжением, может превзойти самые смелые ожидания.
Анализ риска в настоящее время каждый технологический процесс контролируется информационными технологиями — будь то даже регулировка дорожного движения, малейшее нарушение в которой вызовет серьезные проблемы. Активное использование технологий сделало цивилизацию зависимой,а следовательно, уязвимой. Поэтому предугадать последствия кибератаки невозможно. Многие страны обеспокоились безопасностью своих информационных систем и вписали ее в национальную стратегию обороны. Де-факто интернет-пространство стало новой сферой ведения военных действий. В США для наступательных действий и защиты важных объектов от киберугроз создано киберкомандование. В России в 2014 году созданы войска информационной безопасности (кибервойска). В Китае также состоят на службе порядка 20 тысяч хакеров. Кроме указанных стран, к кибервойне также готовятся Иран, Израиль, европейские страны. Основная цель кибервойск — защита инфраструктуры страны и асимметричное воздействие на противников, которое представляет собой нанесение вреда с использованием всех доступных технологий.

Список использованных источников

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум / под ред. Поляковой Т.А., Стрельцова А.А. – М.: Юрайт, 2017. – 325 с.

АВТОМАТИЗАЦИЯ ПРОЦЕССОВ РЕГИСТРАЦИИ И КОММУНИКАЦИИ В СРЕДЕ INTERNET УЧАСТНИКОВ КОНФЕРЕНЦИЙ, СЕМИНАРОВ, ДИСТАНЦИОННЫХ ОЛИМПИАД

Богданова Юлиана Сергеевна, студентка 3 курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

На протяжении долгого времени широкий спектр различных групп и сообществ заинтересован в проведении конференций для обсуждения волнующих тем мирового, регионального или производственного масштаба. Ученые, экономисты, политики осуществляют мероприятия подобного рода. Охват все продолжает расти. Стоит отметить, что молодое поколение получает ценнейший набор знаний и умений в ходе проведения собраний. Школьникам и студентам прививают любовь к семинарам, активному участию в олимпиадах, а также предоставляют возможность студенческим советам организовывать свои собственные мини-конференции ради решения вопросов на уровне колледжа или университета. Требуется интенсивная работа и огромная отдача всех сторон, задействованных в ней, для осуществления мероприятия на высококачественном уровне. В особенности важна подготовка организаторов, чтобы оправдать ожидания участников и укрепить статус конференции.

Актуальность выбранной темы определяется переходом на дистанционный режим большинства аспектов жизни современного человека: работа, учеба, деловые встречи, конференции, олимпиады. Из этого вытекает необходимость разработки ИС, автоматизирующей регистрацию участников на все подобные собрания.

Предметной областью научно-исследовательской работы является регистрация участников собраний, проводимых в онлайн-режиме в сети Internet. Рост популярности такого рода деятельности также свидетельствует о необходимости создания информационной системы, позволяющей наладить автоматизацию регистрации всех желающих участвовать, в целях снижения ошибок по человеческому фактору. Персональные данные вводятся непосредственно самим пользователем, что значительно снижает объем и время их обработки. Необходимо удовлетворить пользовательские потребности в удобном, а главное понятном интерфейсе, корректной работе форм регистрации и информации, и также реализовать обратную связь участникам. Главной целью поставили отслеживание организатором гостей мероприятия.

Моделирование основных и вспомогательных процессов осуществляется с помощью языка UML. Язык моделирования – это набор графических обозначений, используемых для описания моделей в процессе проектирования. Нотация представляет собой набор графических объектов, используемых в модели, и является синтаксисом языка моделирования. Язык моделирования, с одной стороны, должен понимать решения планировщиков, с другой стороны, обеспечить планировщикам достаточно средств и четкое определение дизайнерских решений, реализуя их в виде программных систем, образуя целостную систему [3]. С помощью языка UML можно смоделировать диаграммы классов, компонентов, развертывания, объектов, деятельности, автомата, сценариев использования, последовательности, обзора взаимодействия.

На диаграмме компонентов рисунка 1 представлена информационная система в качестве пакета модулей. Программный модуль – модуль, содержащий все классы ИС и их методы. Модуль взаимодействия с БД – модуль для работы с базой данных. Включает в себя следующие основные компоненты:

• рабочая среда – окно, состоящее из модулей, с которыми могут работать пользователи в зависимости от их права доступа;

• модуль хранения информации о мероприятиях (база данных) – изменяющийся архив с фильтрами на вывод;

• модуль создания новых мероприятий – позволяет пользователю вносить записи с данными о предстоящих собраниях;

• модуль поиска мероприятий – облегчает посетителям поиск нужных им собраний по нескольким категориям ввода информации;

• модуль хранения информации о регистрации (база данных) – неизменный архив, который соединяет в одну запись информацию организатора и посетителя;

• модуль хранения информации о посетителях – неизменный архив, хранящий персональные данные зарегистрированного посетителя;

• модуль формирования отчетов – получает информацию из двух модулей, рассмотренных выше, формирует отчет и отправляет его пользователю, сделавшему запрос;

• модуль хранения информации о пользователях (база данных) – архив с учетными записями зарегистрированных пользователей;

• модуль поиска пользователя (база данных) – осуществляет проверку наличия учетной записи в базе данных при выполнении авторизации или регистрации;

• модуль регистрации новых пользователей – обрабатывает запрос на добавление пользователя в базу, если модуль поиска предварительно не нашел уже имеющуюся подобную учетную запись;

• модуль технической поддержки – позволяет обычным пользователям приложения получать обратную связь от администрации

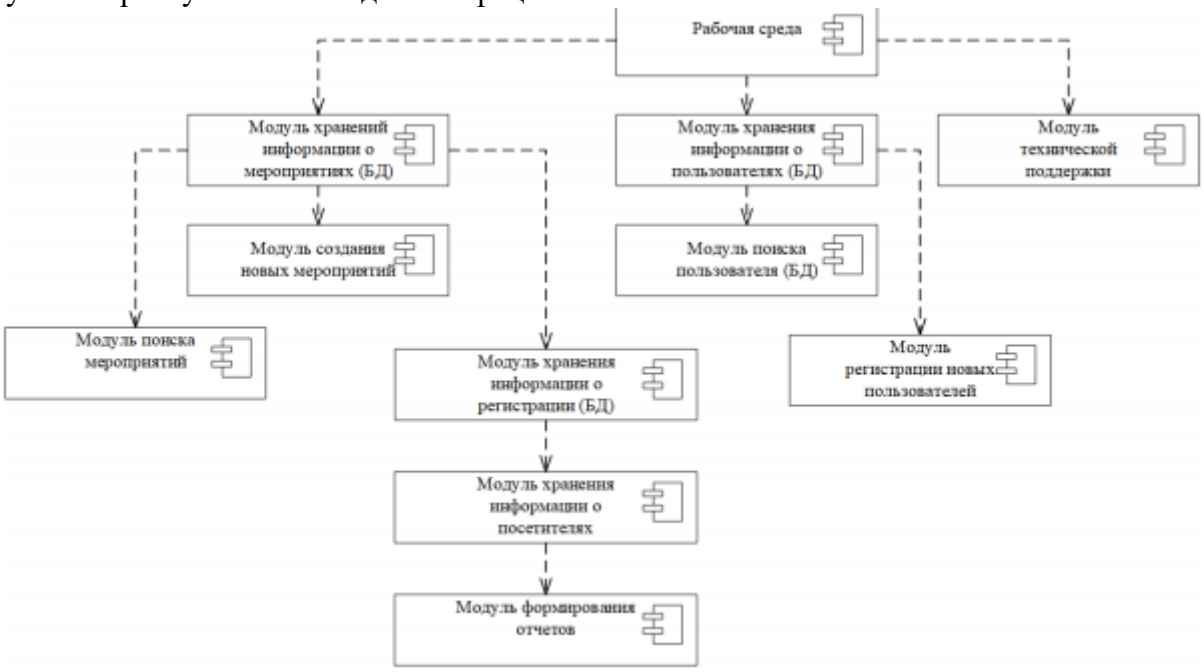


Рисунок 1 – Диаграмма компонентов

Диаграмма классов, изображенная на рисунке 2, служит для демонстрации атрибутов, методов и зависимостей между несколькими различными классами.

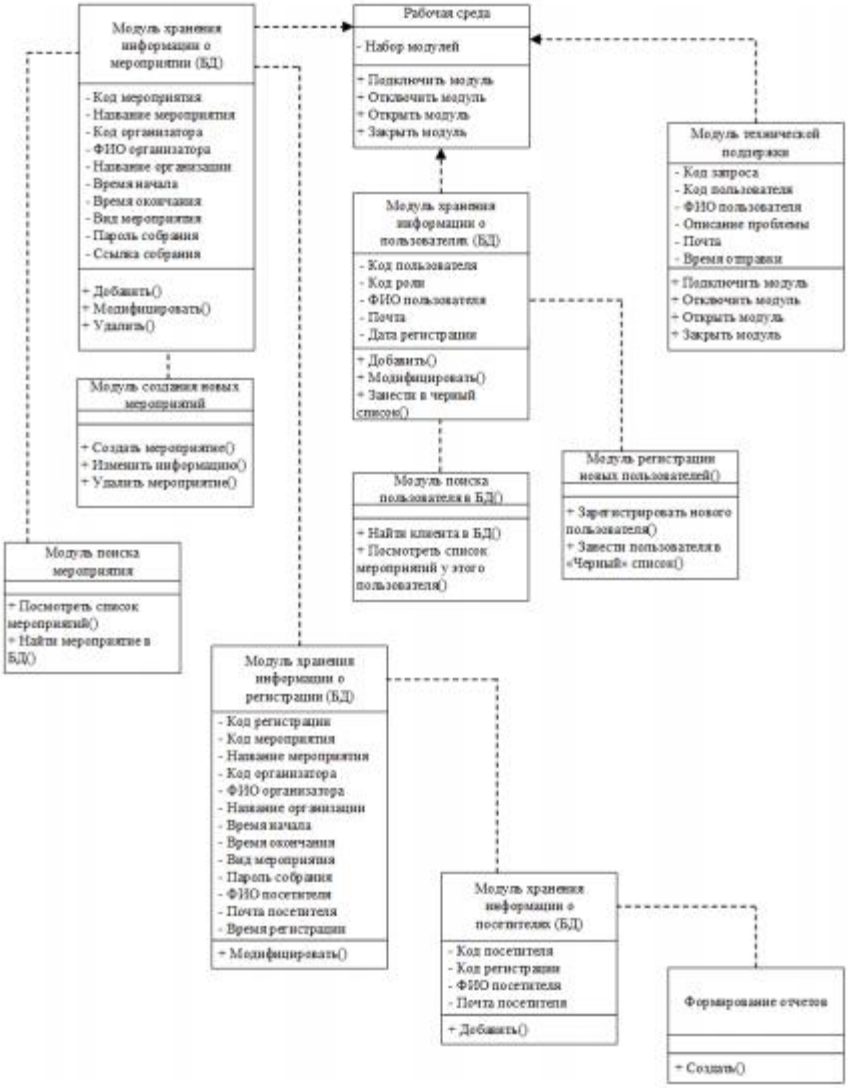
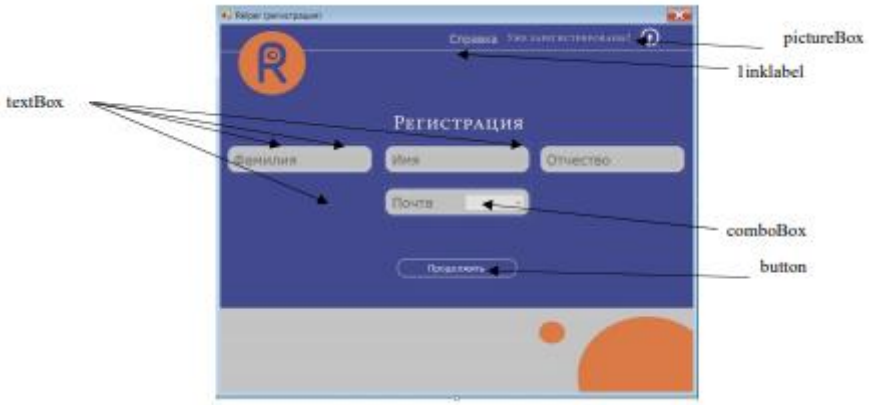


Рисунок 2 – Диаграмма классов

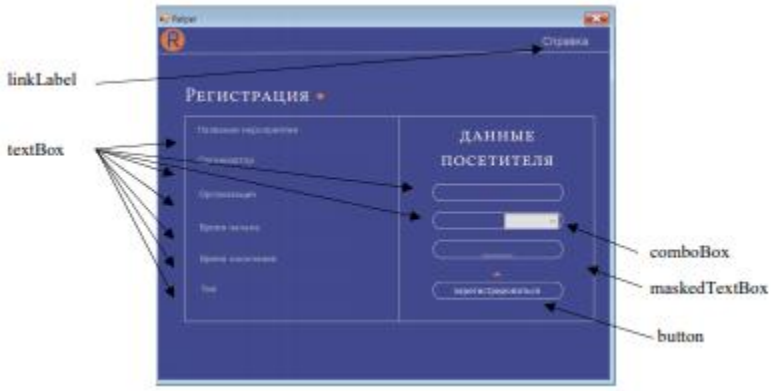
К задачам разрабатываемой ИС относятся:

• регистрация пользователей в приложении;

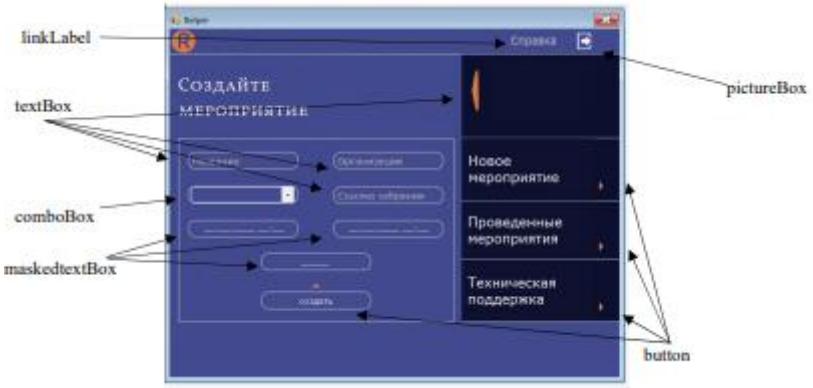


• возможность опубликовать информацию о предстоящем мероприятии;

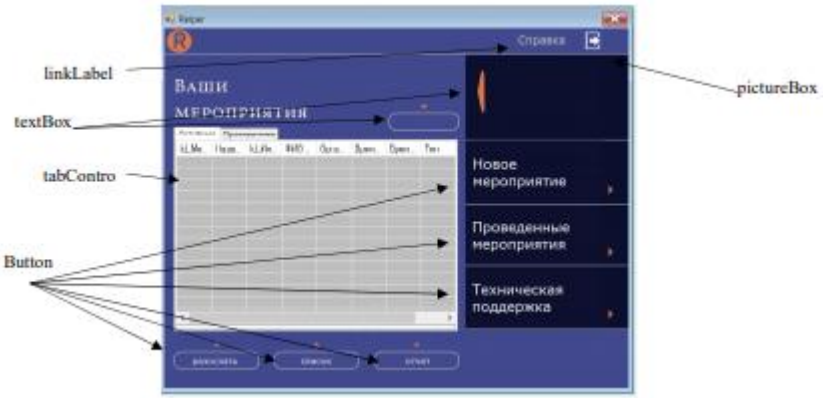
• регистрация желающих посетить мероприятие;



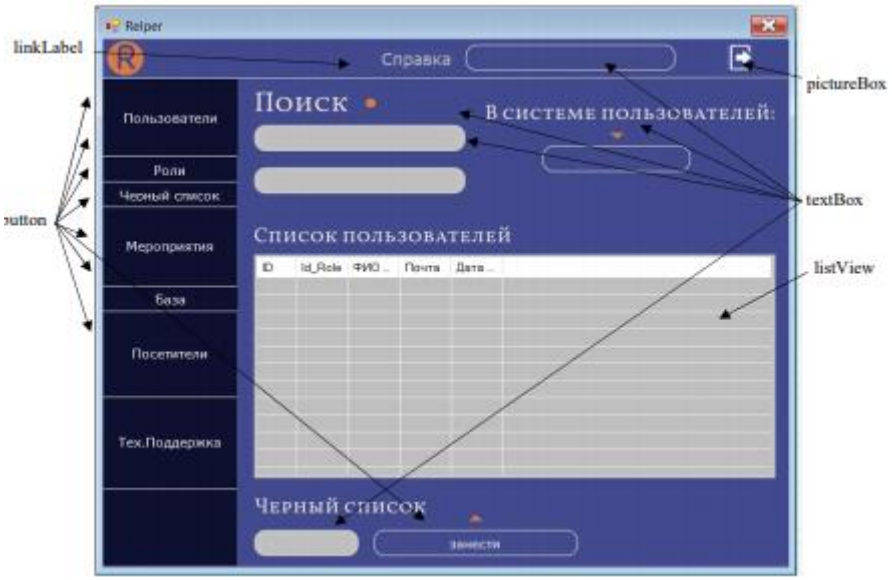
• автоматическая отправка на почту зарегистрированным посетителям ссылок на собрание; обеспечение возможности обратной связи от модератора приложения;



• добавление, удаление и модификация данных со стороны администратора; подсчет посетивших мероприятие участников;



• формирование отчета с ФИО посетителей мероприятия по запросу организатора; проводить поиск мероприятия или организатора в списках; занесение пользователя в «Черный» список по желанию администратора.



В завершении следует отметить, что разработанная автоматизированная система универсальна, и может быть интегрирована в web-приложение для охвата большего числа пользователей.

Список использованных источников

1. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова–Виснадул; под ред. Л.Г. Гагариной. – Москва: ФОРУМ: ИНФРА–М, 2020. – 400 с. – (Среднее профессиональное образование). – ISBN 978–5–8199–0812–9. Текст: электронный. – URL: https://znanium.com/catalog/product/1067012
2. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В.А. Гвоздева, И.Ю. Лаврентьева. – Москва: ИД «ФОРУМ»: ИНФРА–М, 2018. – 318 с. – (Среднее профессиональное образование). – ISBN 978-5-8199-0705-4. – Текст: электронный. – URL: https://znanium.com/catalog/product/922734
3. Пальмов, С. В. Методы и средства моделирования программного обеспечения: конспект лекций / С. В. Пальмов. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. – 105 с. – ISBN 2227-8397. – Текст: электронный // Электронно–библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/71855.html
4. Двумерная графика на C#, классы Graphics, Pen и Brush [Электронный ресурс]: https://c-sharp.pro/?p=47
5. Информация по пакетам NuGet в C# [Электронный ресурс]: https://qna.habr.com/q/285234

РАЗРАБОТКА ИС ПО ОРГАНИЗАЦИИ И ИСПОЛЬЗОВАНИЮ РЕСУРСОВ БИБЛИОТЕКИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

Боева Кристина Николаевна, студентка 4-го курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Работа в библиотеке — это сложный процесс, где применяются информационные технологии. Работники используют специальную систему для того, чтобы внести в онлайн каталог библиотеки информацию о какой-либо книге. Несмотря на это персонал библиотеки также продолжает работать с бумажными носителями. Например, при выдаче книг студентам, вся информация (кому выдана, какая книга, когда выдана) заносится в формуляр. При сдаче книги сотруднику также необходимо внести определённые пометки о том, что книга сдана. Книги, как правило, выдаются на одни-два семестра. Практически в конце каждого семестра библиотекарю нужно составить список должников – тех, кто не сдал книгу вовремя. Для этого нужно просмотреть формуляры, выписать всех должников и составить некоторый отчёт. Весь этот процесс занимает много времени. В настоящее время бумажные носители уже изжили себя и постепенно отходят на второй план.

В связи с этими проблемами к разработке предлагается информационная система организации и использования ресурсов библиотеки для автоматизации работы персонала.

Данная информационная система будет осуществлять учёт ресурсов библиотеки, учёт студентов, которые взяли книги, а также учёт должников. Информационная система позволит быстро и удобно просматривать всю основную информацию о книгах, студентах и сотрудниках.

Объектом исследования является деятельность библиотеки.

Предметом научно-исследовательской работы является информационная система организации и использования ресурсов библиотеки.

Существует большое количество методов исследования. Методы можно разделить на две группы – общие методы и специальные.

В данной работе используются следующие методы исследования:

1. Поиск информации. На данном этапе необходимо найти и просмотреть информацию о предметной области.
2. Анализ. На данном этапе работы выделяются отдельные части и рассматривается основная информация предметной области для детального изучения.
3. Синтез. На данном этапе работы складывается общая структура системы.
4. Обработка результатов исследования.

Для отображения работ и данных предметной области используется диаграмма потоков данных, которая преобразует входные данные процесса в выходные, а также выявляет отношения между этими процессами. Диаграмма входной и выходной информации и разрабатываемой системы представлена на рисунке 1.

В разрабатываемой информационной системе в функциональную подсистему входят:

- вывод информации о студентах;
- вывод информации о сотрудниках;
- вывод информации о книгах;
- вывод информации о выдачах;
- вывод информации о должниках;
- хранение информации.

В обеспечивающую подсистему входят:

- информационное обеспечение;

– программное обеспечение;
– техническое обеспечение;
– организационное обеспечение.

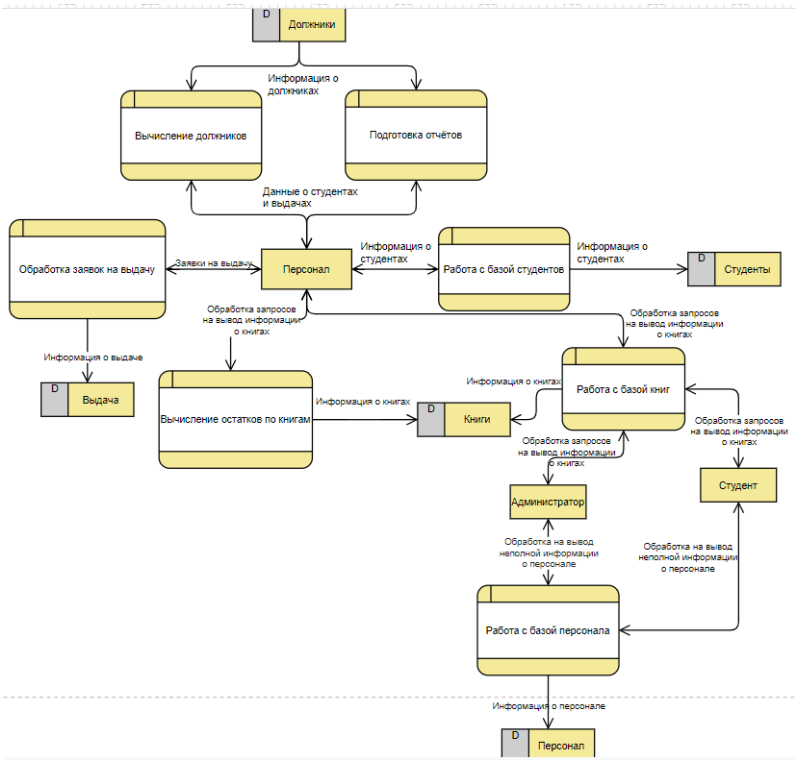


Рисунок 1 - Диаграмма потоков данных

Задачами данной информационной системы являются:
1. Предоставление удобного интерфейса.
2. Хранение информации.
3. Поиск информации.
4. Составление отчётов.

Функциями данной информационной системы являются:
1. Хранение информации.
2. Сбор информации.
3. Автоматизированный поиск информации.
4. Выборка информации по конкретному значению.
5. Составление отчётов.

На рисунке 2 представлена схема данных.

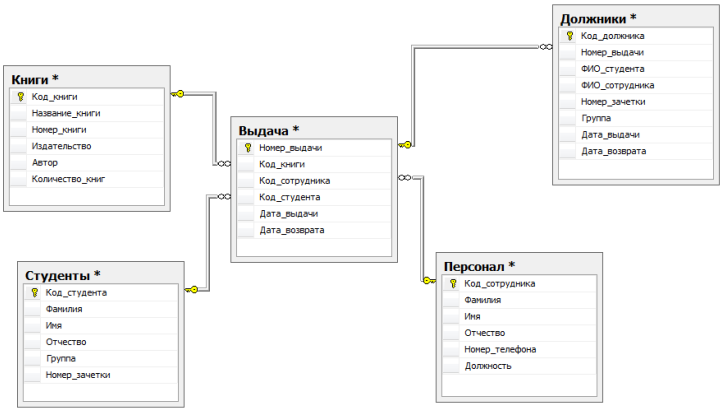


Рисунок 2 – Схема данных

Для создания базы данных была выбрана СУБД MS SQL Server. Это система управления реляционными базами данных, разработанная корпорацией Microsoft.

Для разработки клиентского приложения (программы) была выбрана среда Visual Studio и язык программирования C#, которые позволяют внедрять в систему большое число функций, создать удобный интерфейс и обеспечить безопасность работы пользователя.

После создания БД была произведена разработка интерфейса приложения, через который пользователи (сотрудники предприятия) смогут обращаться к системе.

Защита информации от несанкционированного доступа является важной составляющей каждой информационной системы. От этого зависит не только работа самого приложения, но и будущее предприятия и его сотрудников. Причем создание защиты должно быть реализовано не только в приложении, которым будет пользоваться сотрудник предприятия, но и на сервере, где хранятся все данные. Для этих целей на сервере используется прозрачное шифрование данных. Прозрачное шифрование данных (TDE) помогает защитить базу данных SQL Azure, Azure SQL Управляемый экземпляр и хранилище данных Azure от угроз вредоносной автономной активности, шифруя неактивные данные. Выполняется шифрование и расшифровка базы данных, связанных резервных копий и неактивных файлов журналов транзакций в реальном времени без необходимости изменения приложения. В Azure для TDE ключ шифрования базы данных по умолчанию защищается встроенным сертификатом сервера. Встроенный сертификат сервера уникален для каждого сервера, а используемый алгоритм шифрования — AES 256.

С помощью TDE выполняется шифрование и расшифровка ввода-вывода на уровне страниц данных в реальном времени. Каждая страница расшифровывается при считывании в память, а затем снова шифруется перед записью на диск [7].

Кроме того, для защиты данных пользователя на каждом компьютере предусмотрен исключительный вход по учетной записи Microsoft, которая имеется у каждого сотрудника предприятия и через которую они общаются по почте [4].

Результатом выполнения научно-исследовательской работы является разработанная ИС.

Список использованных источников

1. Бабаш А., Баранова Е., Ларин Д. «Информационная безопасность. История защиты информации в России», 2017., 315 с.
2. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. – М.: ФОРУМ: ИНФРА-М, 2017. – 368с.
3. Козлов А. Д., Лекае В. А., Шаповалова М. С. Методы анализа предметных областей. Учебное пособие – Москва: РГГУ, 2018 – 201 с.
4. Microsoft: [Электронный ресурс]. - https://docs.microsoft.com/ru-ru/ (дата обращения: 20.11.19)
5. Портал электронного обучения ОПК СТИ НИТУ «МИСиС»: [Электронный ресурс]. – http://www.unami.ru/ (дата обращения: 05.04.2021)
6. Сайт для программистов C#: [Электронный ресурс]. – http://www.programmer-lib.ru/csharp.php (дата обращения: 05.04.2021)
7. Шарп Д., Microsoft Visual C#. Подробное руководство 8-е издание – Санкт-Петербург, 2017 – 848 с.
8. НЛМК ИТ: [Электронный ресурс]. - https://it.nlmk.com/ru/about/group-structure/ (дата обращения: 05.04.2021)
9. Универсальная система учета (УСУ): [Электронный ресурс]. - http://usu.kz/index.php (дата обращения: 05.04.2021)

ПРОВЕДЕНИЕ АНАЛИЗА ДЕЛОВОЙ АКТИВНОСТИ И КОНКУРЕНТОСПОСОБНОСТИ ПРЕДПРИЯТИЯ С ИСПОЛЬЗОВАНИЕМ СОВРЕМЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Гойдин Вадим Андреевич, студент 3-го курса,
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Принято считать, что любое современное предприятие, цель которого развиваться и получать прибыль, сможет добиться результативных показателей только путем автоматизации большинства процессов. И в современных условиях цифровизации, движение по пути данной тенденции, является достаточно актуальным.

Стоит отметить, что деловая активность предприятий является одним из центральных факторов эффективности рыночной экономики. Критерии его оценки часто суммируются в источниках особенностей финансового положения предприятий. При этом такая оценка необходима и на макроуровне, которая имеет обязательный характер в большинстве стран мира. Конкурентоспособность коммерческого предприятия проявляется в показателях его развития, а также в достижении установленных коммерческих целей. Все эти данные отражают естественные и ценовые показатели, эффективное использование экономического потенциала, а также расширение рынков реализации для своей продукции. Так же деловая активность является важным фактором, характеризующим финансовую стабильность каждого предприятия. На этот фактор влияют: стабильность экономического роста, количество филиалов предприятия, количество работников, соблюдение установленных темпов развития предприятия, степень завершения принятой работы, уровень эффективности использования имеющихся производственных ресурсов, широта рынков сбыта продукции компании, в том числе наличие экспортных поставок, а также наличие конкретных перспектив развития предприятия.

Объектом цифровизации, в качестве примера автоматизации анализа процессов предприятия, можно считать предприятие автомобильной промышленности. Зачастую, принцип работы данных предприятий достаточно прост: первоочередная задача – произвести продукцию в виде автомобилей, заключить договор о поставках с заказчиком и провести логистику непосредственно к ресейлеру, для дальнейшей розничной реализации продукции. Зачастую у многих крупных автомобильных компаний имеются десятки крупных заводов по всему миру. Все они являются поставщиками продукции, а также имеют сотрудников и логистические пути реализации продукции. Следственно, на предприятии появляется большое количество показателей по данным по оплате труда, информации о продукции, о заказчиках, о сотрудниках, о логистике, которые следует автоматизировать. Так же по истечению всех процессов, предприятие имеет дело с финансовыми показателями. Когда век цифры был только в перспективе, каждый филиал предприятия имел огромные бухгалтерские и статистические отделы, содержание которых было затратным и малоэффективным. Но в нынешний век цифровизации, считается актуальным автоматизация финансовых показателей, не только статистических данных, но и оплаты счетов за продукцию, создание скидочных программ и программ лояльности, а также создания программных средств для быстрого и эффективного построения логистических планов поставок продукции. Все эти показатели напрямую являются объектами анализа деловой активности и конкурентоспособности предприятия с использованием современных информационных систем.

Для достижения поставленной цели необходима разработка базы данных, которая будет хранить данные и информацию, а также приложение, которое будет иметь

эргономичный интерфейс, получать данные из базы данных, а также отвечать всем требованиям по анализу деловой активности и конкурентоспособности предприятия

В качестве входной информации выступают следующие информационные потоки данных:

- данные о продукции;
- данные о заказчиках;
- информация о сети предприятий компании и их деятельности;
- данные о логистике;
- данные о заключенных сделках.
- данные о сотрудниках
- данные об оплате труда

В качестве выходной информации, при учете всех входных данных, для данной предметной области являются рассчитанные финансовые показатели предприятий, которые являются экономическим синонимом деловой активности и конкурентоспособности.

На рисунке 1 представлена диаграмма вариантов, которая описывает главный процесс последовательности заказа, производства и реализации продукции предприятия

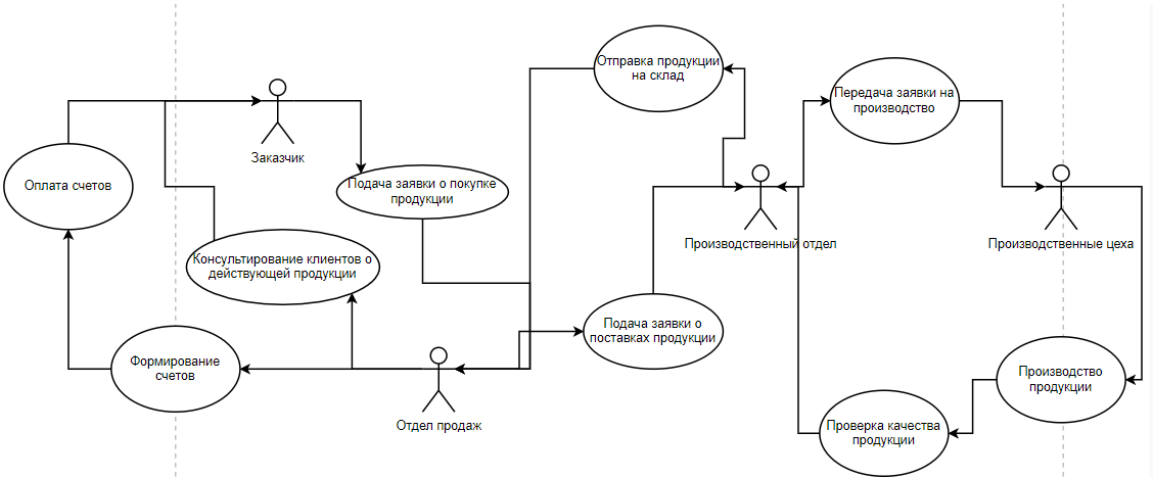


Рисунок 1 – Диаграмма вариантов первоочередных процессов предприятия предметной области

Так же следует представить диаграмму потоков данных, которая более точно описывает процесс анализа деловой активности и конкурентоспособности предприятия, а так же его автоматизации.

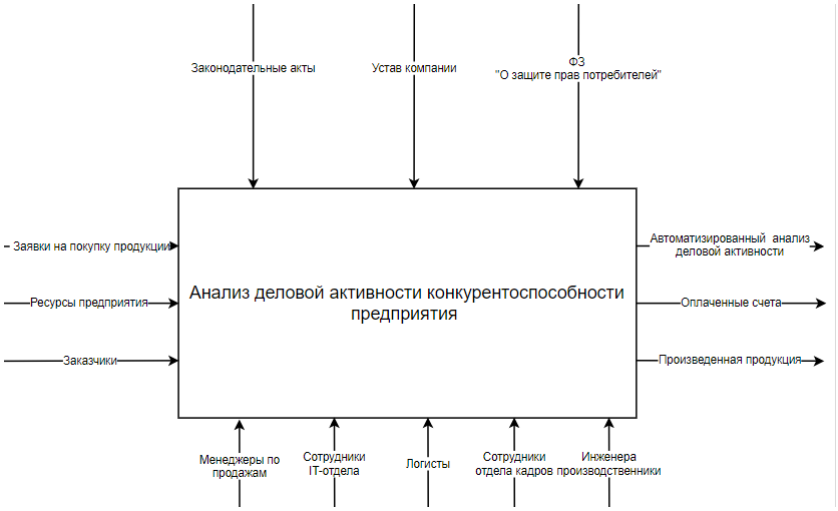


Рисунок 2 – Диаграмма декомпозиции

В заключении стоит отметить, что анализ деловой активности и конкурентоспособности предприятия с использованием современных информационных систем является наиболее быстрым, рациональным и эффективным.

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. – М.: ФОРУМ: ИНФРА-М, 2017. – 368с.
2. Универсальная система учета (УСУ): [Электронный ресурс]. - http://usu.kz/index.php (дата обращения: 05.04.2021)

АВТОМАТИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ УЧЕТА И МОНИТОРИНГА ПРОДУКЦИИ ПРЕДПРИЯТИЯ

Демахин Данила Сергеевич, студент первого курса
Цвентарных Владимир Алексеевич, студент первого курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Аннотация: В данной статье рассматривается проблема учета и мониторинга плодово-ягодных культур. В настоящее время большинство предприятий для ведения учета используют специализированные программы, такие как 1С. Но, как привило, они не учитывают специфику каждого предприятия, а предоставляют набор универсальных средств, которые позволяют полностью автоматизировать бизнес-процессы предприятия.

Ключевые слова: база данных, информационная система, СУБД.

Актуальность разработки информационной системы заключается в повышении эффективности процесса оформления и продажи продукции.

Целью научно-исследовательской работы является проектирование информационной системы учета и мониторинга плодово-ягодных культур на предприятии.

Для достижения поставленной цели необходимо выполнить следующие задачи:

- сформулировать цель разработки информационной системы;
- собрать данные для анализа использования и функционирования ИС;
- провести анализ предметной области;
- построить инфологическую модель данных;
- на основании разработанной ИЛМ создать базу данных в среде выбранной СУБД;
- разработать алгоритмы работы программы;
- разработать эргономичный пользовательский интерфейс;
- разработать справочную систему;
- проанализировать возможные способы обеспечения информационной безопасности данных системы;
- оценить ИС с точки зрения возможностей ее дальнейшего развития;
- выполнить демонстрацию разработанной ИС в соответствии с заданием с целью проверки соответствия результатов работ.

Входная информация представляет собой информацию, поступающая извне и использующаяся как первичная информация для реализации экономических и управленческих функций и задач [3].

Входной информацией разрабатываемой системы являются:

- данные о продуктах предприятия;
- данные о клиентах, взаимодействующих с предприятием.

Выходная информация — это полученная информация на основе входной информации. Выходная информация включает данные предметной области, полученные в результате автоматизированной обработки[3].

Выходными данными являются:

- отчеты;
- статистические данные, позволяющие визуализировать наиболее важные параметры рассматриваемой предметной области.

Перед началом проектирования информационной системы необходимо разработать базу данных, в которой будет храниться необходимая информация в виде двумерных таблиц. База данных будет реализована посредством реляционной СУБД, которые предназначены для управления, создания и поддержания баз данных. В данной работе была выбрана СУБД

Microsoft SQL Server 2016. Microsoft SQL Server обладает всеми качествами, необходимыми для реализации ключевых требований к СУБД, предъявленными заказчиком, а именно – производительностью, стабильностью и возможностью масштабирования. Microsoft SQL Server имеет бесплатный выпуск – SQL Server Express для разработчиков и независимых поставщиков [1].

Достоинства:

- обеспечивает интеграцию с Microsoft Office;
- гарантирует повышенную безопасность;
- гарантирует производительность средств разработки;
- содержит более мощные инструменты бизнес-аналитики.

Информационная система была разработана в среде программирования Microsoft Visual Studio.

Microsoft Visual Studio представляет собой интегрированную среду разработки различных классов приложений для операционной системы Windows, а также имеется возможность создания приложений для ОС Linux, MacOS и мобильных операционных систем [1].

В ходе проектирования информационной системы был разработан графический интерфейс посредством экранных форм.

Так на рисунке 1 представлена форма нового заказа.

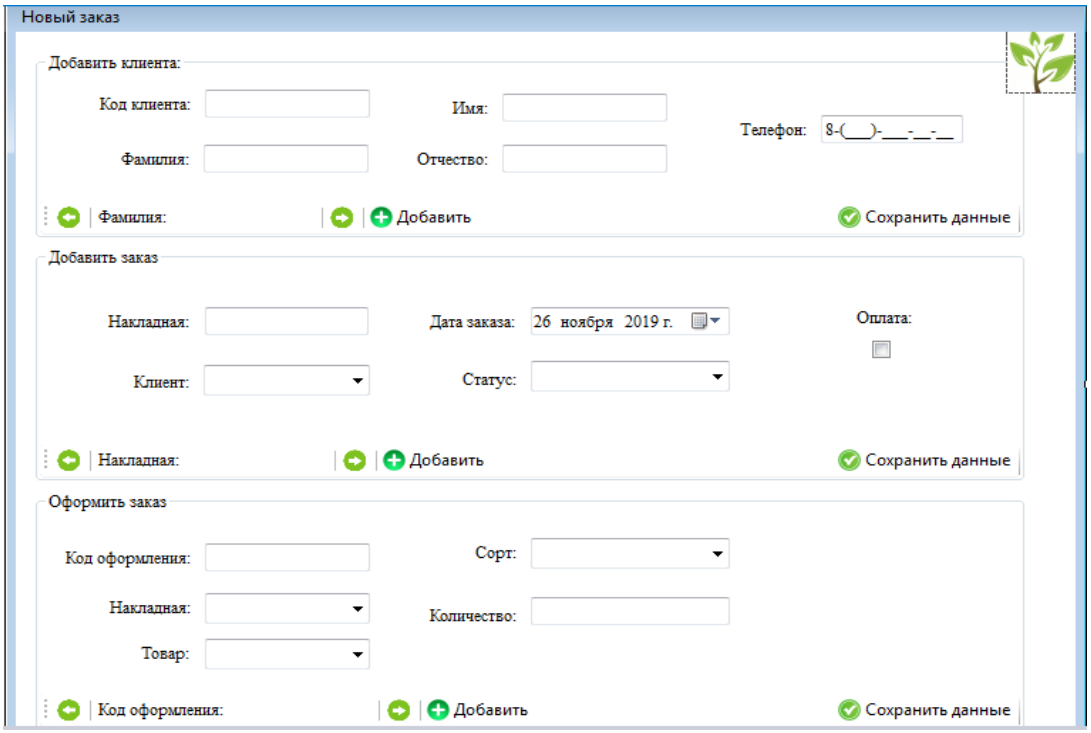


Рисунок 1 - Форма оформления нового заказа

На форме размещены следующие компоненты:

1 – GroupBox;

2 – PictureBox.

На рисунке 2 представлена форма мониторинга. На протяжении сезона графики отображают прибыль, а также имеется возможность отследить спрос на каждую категорию продукции.

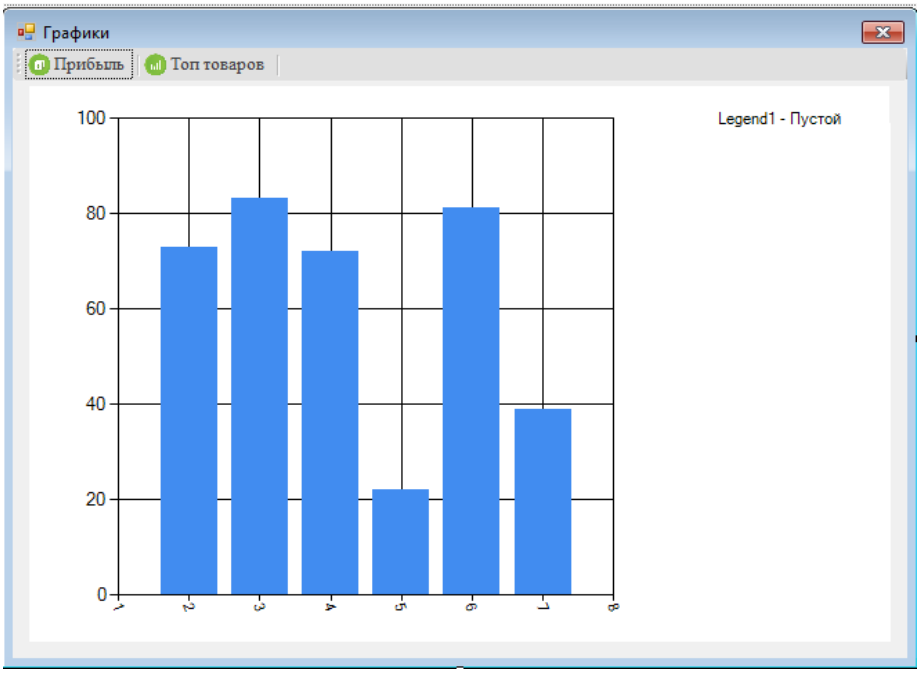


Рисунок 2- Форма мониторинга

Для обеспечения информационной безопасности были приняты следующие меры:

- установлены антивирусные программы;
- настроен брандмауэр;
- обеспечено разграничение доступа к данным в клиентском приложении;

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие/ А.В Васильков, И.А. Васильков. - М: ФОРУМ: ИНФА-М,2017. - 384 с.

2. Конова Е.А., Поллак Г.А. Язык С++: Учебное пособие. - 4-е изд, стер. - СПб.: Издательство «Лань», 2019. - 384 с.

3. Немцова Т.И. Программирование на языке высокого уровня программирование на языке С++: учебное пособие.

4. Сайт для программистов C#: [Электронный ресурс]. - http://www.programmerlib.ru/csharp.php

5. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. -324 с.:ил.

ИНФОРМАЦИОННАЯ СИСТЕМА УЧЕТА МИКРОКЛИМАТА ПОМЕЩЕНИЯ

Думанский Дмитрий Александрович, студент 3-го курса
Научный руководитель Артюхина Дарья Дмитриевна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В наше время трудно представить свою жизнь без новых технологий, инноваций и интернета. Информационные технологии внедрены практически в каждую область жизни. На каждом государственном или частном предприятии, либо учреждении имеется свой сервер, база данных упрощающие работу организации. Организм человека во многом зависит от внешних условий. Микроклимат помещения, в котором человек находится продолжительное время, влияет на формирование иммунитета, работоспособность и ощущение комфорта.

В процессе исследования было принято решение разработать информационную систему, которая будет позволять автоматизировать процесс учёта микроклимата в помещении.

При проектировании устройств часто возникает задача контроля температуры внутренних модулей или температуры внутри корпуса, а также модулей влажности. В большинстве случаев обработка данных, полученных с сенсора, может быть реализована непосредственно на имеющемся вычислительном узле как дополнительная функция. Цифровые системы измерения температуры сегодня широко применяются в связи с развитием цифровой микроэлементной элементной базы, в частности программируемых интегральных логических микросхем (ПЛИС). При этом особый интерес представляют датчики, которые формируют результат измерения в цифровой или частотной форме. Из существующих температурных датчиков, таких как резистивные термодатчики, термопары, полупроводниковые датчики в качестве сенсора следящей системы контроля температуры используется полупроводниковый термодатчик фирмы Analog Devices TMP03 с частотным выходом.

Данный датчик является доступным, точным (однако точность полупроводниковых датчиков уступает точности термопар) и обладает дополнительным достоинством с точки зрения корпуса, поскольку может быть размещен даже в отверстии внутри твердого тела для измерения его температуры. Выбранный датчик можно размещать на кристаллах интегральных микросхем.

В ходе выполнения работы была реализована следящая система контроля температуры на базе оригинального устройства, которая отличается следящим выполнением функционального множительно-делительного преобразования с использованием только операций «инкремент» и «декремент». Система обладает высокой помехоустойчивостью и реализует следящий режим вычислений.

В разработанной информационной системе осуществляется выдача информации по запросу пользователя, при этом формируются выходные документы. Поиск информации заключается в выведении сведения из БД.

Техническое обеспечение представляет собой совокупность используемых технических средств, вычислительных сетей, технологий сетевой обработки данных.

Структуру подсистемы образуют: технические средства сбора и регистрации информации, средства подготовки и передачи данных, средства ввода, обработки и вывода информации и другие.

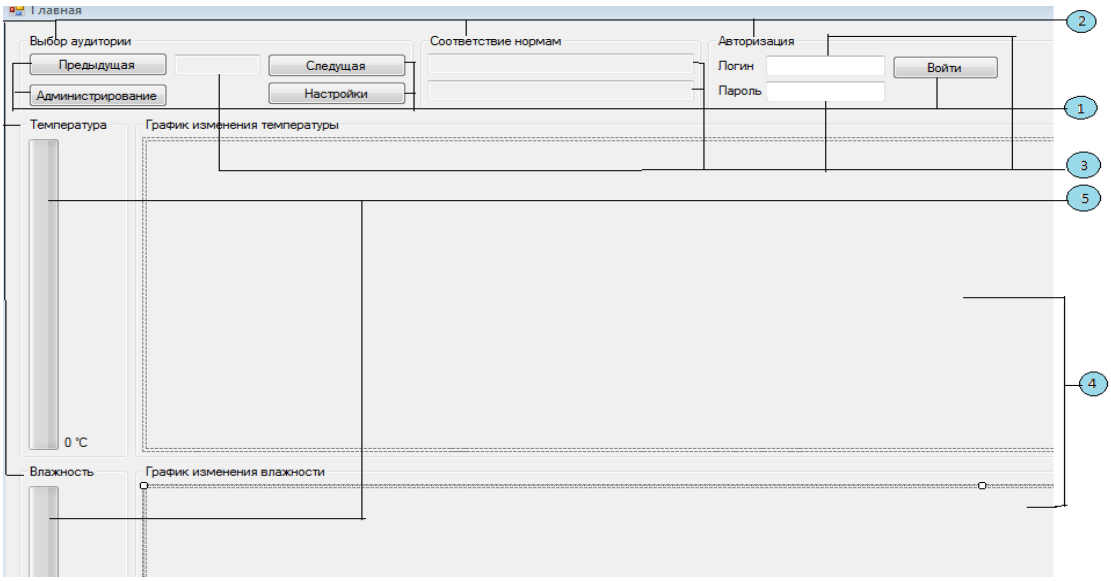


Рисунок 1 – Главная форма ИС, которая включает панель основных настроек (1), подсказки к панели (2), области вывода динамических показателей микроклимата (3), область графического вывода динамических показателей микроклимата (4, 5).

Данная информационная система «считывает» и обрабатывает показатели с датчиков температуры и влажности воздуха и сохраняет их в базе. Если показатели выходят за пределы норм, система «оповещает» пользователей. Вместе с данным оповещением пользователь получает рекомендации по приведению показателей в норму.

На данный момент система реализована и внедрена в одной аудитории Оскольского политехнического колледжа СТИ НИТУ «МИСиС» на отделении информационных технологий. В ближайшем будущем планируется доработать аппаратную и программную части системы, чтобы увеличить охват аудиторий в колледже, где данные будут аккумулироваться в единой системе.

Список использованных источников

1. Соммер, У. Программирование микроконтроллерных плат Arduino/Freeduino / У. Соммер. - СПб.: BHV, 2016. - 256 с.

2. Белов, А.В. Программирование микроконтроллеров для начинающих и не только / А.В. Белов. - СПб.: Наука и техника, 2016. - 352 с.

3. Иванов, В.Б. Программирование микроконтроллеров для начинающих Визуальное проектирование, язык С, ассемблер / В.Б. Иванов. - СПб.: Корона-Век, 2015. - 176 с.

ПРОЕКТИРОВАНИЕ ПРОГРАММНОГО МОДУЛЯ АНАЛИЗА ЗАГРУЖЕННОСТИ АВТОПАРКА

Жуков Максим Рудольфович, студент 4 курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Грузоперевозки являются очень важной частью нашей жизни, именно благодаря ним люди получают большой ассортимент товаров в магазинах. Такое разнообразие товаров с разными ценами позволяет удовлетворить потребности всех экономических слоёв общества.

Актуальность обоснована важностью количества затрачиваемого времени в сфере грузоперевозок. ПО даст возможность ускорить большинство процессов, благодаря своим возможностям работы с информацией.

Объектом исследовательской работы является организация, занимающаяся грузоперевозками и нуждающаяся в учёте перевозок товара с анализом загруженности автопарка для улучшения своих показателей и увеличения конкурентоспособности на рынке среди организаций, занимающихся схожим видом деятельности.

Предметом - создание программного обеспечения с графическим интерфейсом для поддержки процессов учета перевозок товара с анализом загруженности автопарка, призванное автоматизировать рабочие процессы организации.

Грузоперевозки требуют учёта множества различных параметров для эффективной работы. Для того чтобы вести бизнес в сфере грузоперевозок, нужно тщательно учитывать специфику работы различных видов транспорта, а также брать в учёт определённые обстоятельства. Такими обстоятельствами могут быть пробки, расстояние пунктов доставки друг от друга, грузоподъёмность машины, и так далее. Если вести учёт всех этих факторов вручную, то перед отправкой каждого заказа будет затрачиваться огромное количество времени, а чем больше времени затрачивается на заказ, тем ниже конкурентоспособность предприятия, занимающегося грузоперевозками.

Моделирование основных и вспомогательных процессов предметной области является неотъемлемым процессом при создании и проектировании любой информационной системы.

Диаграмма сценария работы предприятия, занимающегося перевозкой товара в рассматриваемой предметной области отражена на Рисунке 1.

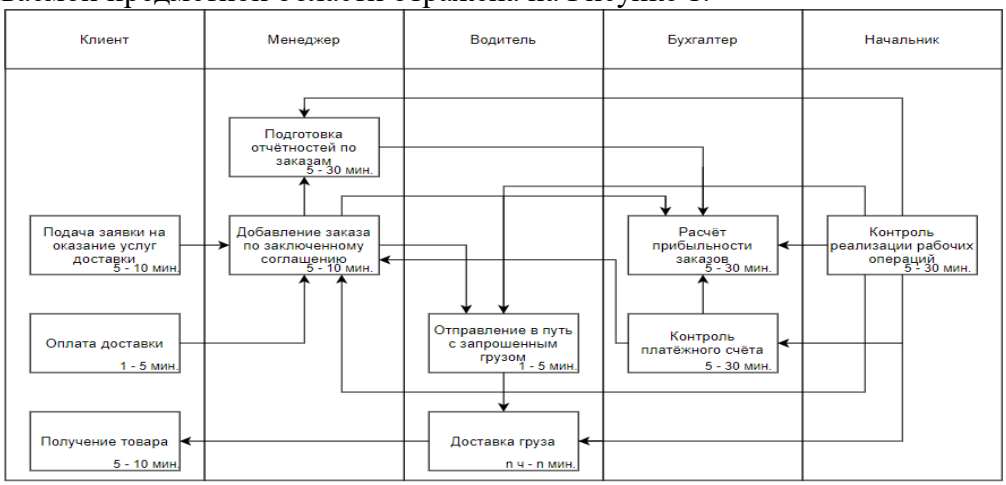


Рисунок 1 – Диаграмма сценария работы предприятия, занимающегося перевозкой товара

Диаграмма компонентов рассматриваемой предметной области представлена на Рисунке 2.

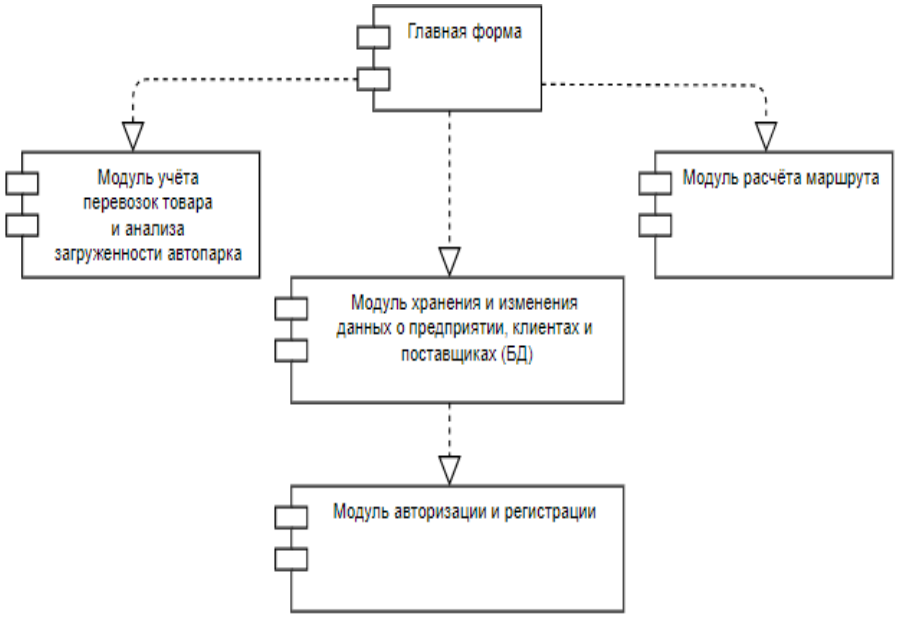


Рисунок 2 – Диаграмма компонентов

На диаграмме компонентов, изображенной на Рисунке 2 система является пакетом, включающим в себя пять основных компонентов:

– главная форма – представляет собой окно, состоящее из модулей, с которыми может работать менеджер;
– модуль учёта перевозок товара и анализа загруженности автопарка – позволяет хранить, добавлять и редактировать заказы, выполняемые организацией, а также изменять статус заказа в зависимости от времени, которое отводилось на его выполнение;
– модуль хранения и изменения данных о предприятии, клиентах и поставщиках (база данных) – постоянно изменяющийся архив со всей необходимой для основных функций менеджера информации;
– модуль расчёта маршрута – позволяет наглядно показать маршрут, построенный между точками отправления и прибытия, а также рассчитать расстояние и время выполнения для заказа;
– модуль авторизации и регистрации – позволяет вносить и редактировать информацию о пользователях, работающих с ИС.

Разработанное приложение имеет следующие формы:

1. Окно «Авторизация», представленное на рисунке 3. Позволяет войти в систему при наличии логина и пароля, или зарегистрироваться новым пользователям.

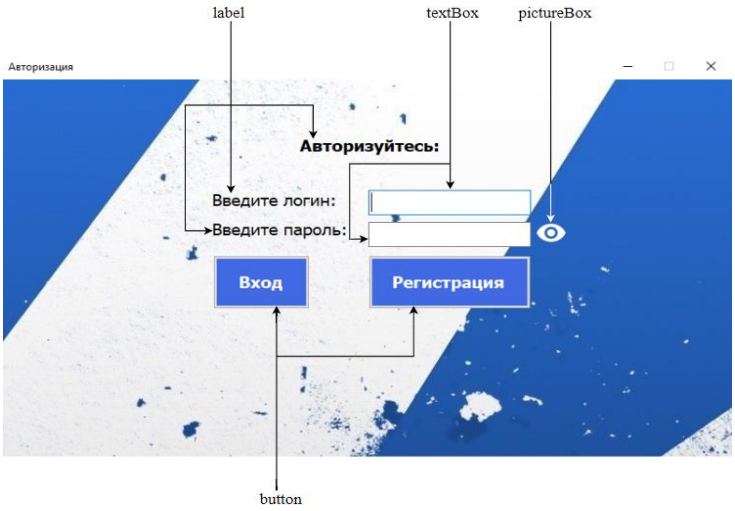


Рисунок 3 – Окно «Авторизация»

2. Окно «Главная форма», предназначена для решения и представления основных процессов и задач программного модуля, представлена на рисунке 4.

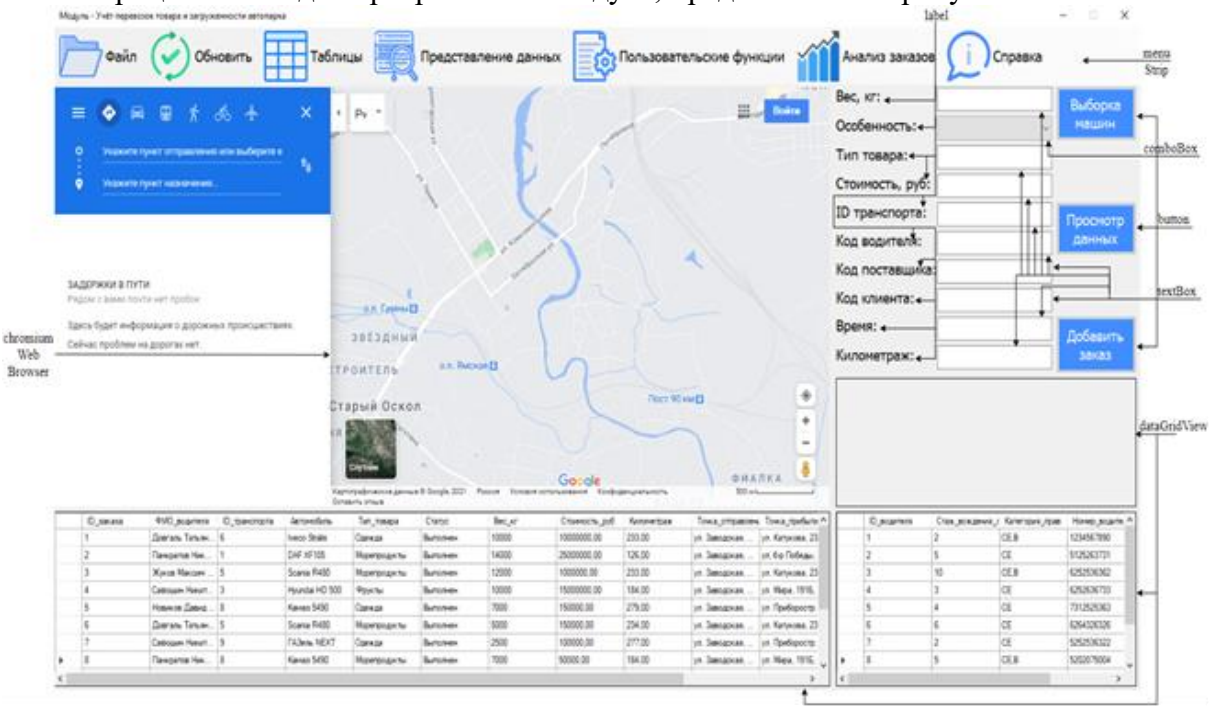


Рисунок 4 – Окно «Главная форма»

В заключении курсовой работы можно сделать вывод, что была разработана система процессов учёта перевозок товара с анализом загруженности автопарка.

Были решены следующие задачи:

- реализована возможность учёта перевозок товара;
- реализована возможность анализа загруженности автопарка;
- реализовано сохранение информации о перевозках в базе данных;
- организовано разграничение прав доступа пользователей к ПО в зависимости от представленных им прав доступа к информации.
- в системе накапливается и хранится статистика о работе предметной области для подготовки сводной отчетности, а также анализа динамики деятельности предметной области;
- клиентам предметной области предоставляется справочная информация по их запросам о производственных заявках.

Список использованных источников

1. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова–Виснадул; под ред. Л.Г. Гагариной. – Москва: ФОРУМ: ИНФРА-М, 2020. – 400 с. – (Среднее профессиональное образование). – ISBN 978–5–8199–0812–9. – Текст: электронный. – URL: https://znanium.com/catalog/product/1067012
2. Пальмов, С. В. Методы и средства моделирования программного обеспечения : конспект лекций / С. В. Пальмов. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. – 105 с. – ISBN 2227-8397. – Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/71855.html
3. Перевозка грузов автомобильным транспортом по России и СНГ [Электронный ресурс]: https://gruzoved.com/
4. Биржа международных перевозок CARGOX [Электронный ресурс]: https://cargox.ru/

ПРОЕКТИРОВАНИЕ СИСТЕМЫ КОНТРОЛЯ И УЧЕТА ЭНЕРГОРЕСУРСОВ

Коренев Александр Михайлович, студент 3-го курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Потребление энергоресурсов в мире непрерывно повышается. В 2000 году количество электроэнергии, вырабатываемой совокупной мощностью всех предприятий, достигла 14.500 млрд кВт*ч. А к 2016 году 24.816 миллиарда киловатт – час. Однако это потребление энергоресурсов осуществляется крайне неравномерно. Примерно 70% мировой энергии потребляют промышленно развитые страны. При неконтролируемом использовании ресурсов их исчерпаемость неизбежна, поэтому большинство промышленных предприятий стремятся оптимизировать использование энергоресурсов.

Актуальность данной работы заключается в разработке системы контроля и учета энергоресурсов для рационального использования энергоресурсов.

Энергоменеджмент – это комплекс мер, используемых в различных сферах потребления энергоресурсов и направленных на повышение энергоэффективности. Однако наличие систем энергоменеджмента на российских предприятиях слабо развито. Это связано с отсутствием понимания того, как работают данные системы и какова сложность и длительность их реализации.

Платформа arduino для проектирования и создания новых устройств очень популярна благодаря открытой архитектуре, множеству библиотек и развитому сообществу. В настоящее время разработка на данной платформе позволяет решать множество задач: работа с датчиками, получающими информацию о состоянии окружающей среды, а также управление исполнительными устройствами 3D – принтера или ЧПУ станка и т.д.

Проектируемая программно-аппаратная платформа позволит осуществлять контроль энергоресурсов и передачу данных на ПК для построения графиков энергопотребления и сохранение полученных данных.

Для осуществления вышеперечисленных функций необходимо разработать аппаратно-техническое обеспечение, которое будет соответствовать требованиям:

- взаимодействие с устройством должно осуществляться с помощью приложения с интуитивно понятным интерфейсом;
- приложение должно поддерживаться ОС Windows;
- устройство должно иметь компактный размер, обеспечивающий мобильность;
- корпус устройства должен состоять из прочных материалов;
- сохранение отчетов.

В таблице 1 представлены характеристики аппаратно-технического устройства.

Таблица 1 - Технические характеристики устройства

Критерии	Описание
Поддерживаемые ОС	Windows 7/10
Энергопотребление	0,100 Вт
Материалы корпуса	Petg пластик
Размер	63 х 35см
Плата	Arduino nano
Сохранение отчетов	в формате CSV

Для создания аппаратно-технического устройства были использованы следующие компоненты:

1. Arduino nano

2. Резисторы
3. Фоторезистор
4. Потенциометр
5. Светодиоды
6. Кабель для подключения устройства

Электрическая схема — это документ, содержащий в виде условных изображений или обозначений составные части изделия, действующие при помощи электрической энергии, и их взаимосвязи. Электрические схемы являются разновидностью схем изделия и обозначаются в шифре основной надписи буквой Э.

Arduino – это электронная платформа с открытым исходным кодом, основанная на простом в использовании аппаратном и программном обеспечении. Конструкция миниатюрной платы Arduino nano такова, что ее можно установить в панельку для микросхем.

Фоторезистор представляет собой переменный резистор, управляемый светом. Фоторезистор имеет очень высокое сопротивление в темноте, но при освещении оно существенно уменьшается в зависимости от силы света, вплоть до всех лишь нескольких сотен ом. Фоторезисторы используются в схемах включения и выключения, активируемых темнотой или светом, а также в светочувствительных схемах детектирования.

Потенциометр – это регулируемый делитель напряжения, предназначенный для регулирования напряжения. Потенциометры изготавливаются разных физических форм, с разными типами резистивных элементов. Некоторые переменные резисторы рассчитаны на частую ручную регулировку и оснащены для удобства ручкой; другие предназначены только для периодической тонкой настройки схемы посредством отвертки (или подобного инструмента с плоским жалом).

Светодиод – полупроводниковый элемент, который создает оптическое излучение при прохождении через него тока в прямом направлении. Подключать светодиод нужно с соблюдением полярности. Для этого необходимо посмотреть на контакты светодиода, длинная ножка соответствует положительному электроду.

В таблице 2 приведен список всех элементов, используемых в процессе проектирования.

Таблица 2 - Используемые компоненты

Наименование	Количество(шт.)
Arduino nano	1
Резистор 10 кОм	1
Резистор 220 Ом	2
Потенциометр 100 кОм	1
Светодиод	2
USB кабель	1

При разработки аппаратно-технического устройства были с проектирована схема макетной платы, представленная на рисунке 1, и электрическая схема, представленная на рисунке 2.

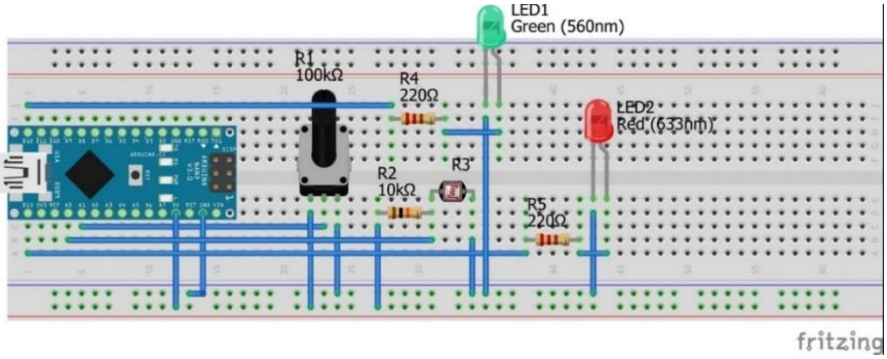


Рисунок 3 – Схема макетной платы

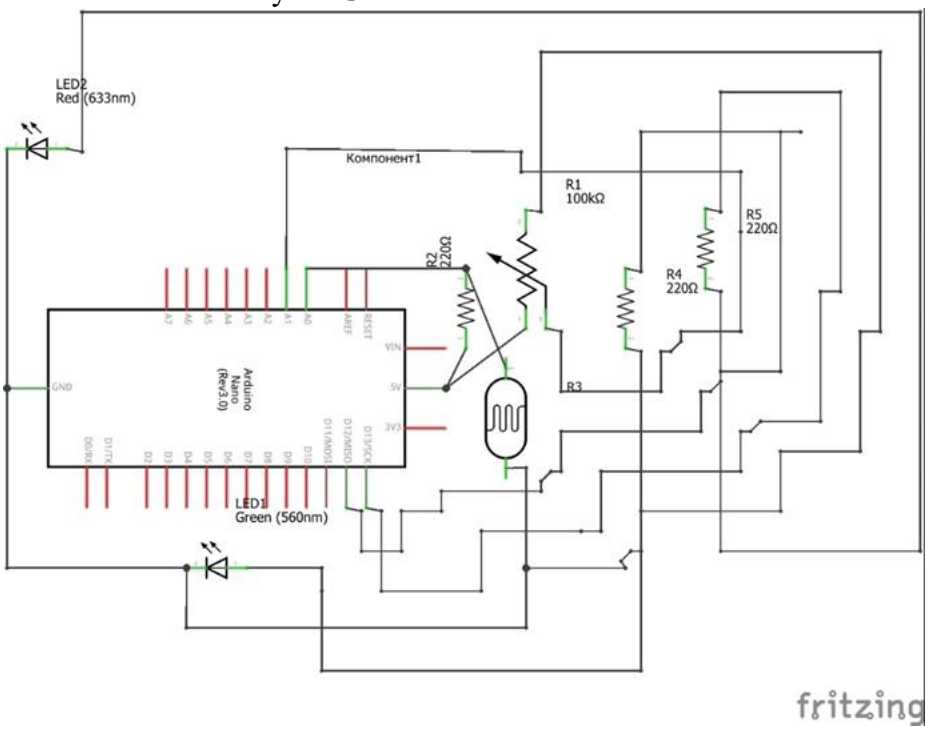


Рисунок 4 – Электрическая схема

Для обеспечения корректной работы было разработана программа, загруженная на плату Arduino.

Результатом выполнения научно-исследовательской работы является готовая аппаратно-техническая разработка и программное приложение для работы с ней.

Список использованных источников

1. Блум Дж. Изучаем Arduino: инструменты и методы технического волшебства. 2-е изд.: пер. с англ. — БХВ-Петербург, 2021—544 с. — ISBN 978-5-9775-6735-0
2. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова-Виснадул ; под ред. Л.Г. Гагариной. — Москва: ФОРУМ: ИНФРА-М, 2020. — 400 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0812-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1067012
3. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В.А. Гвоздева, И.Ю. Лаврентьева. — Москва: ИД «ФОРУМ»: ИНФРА-М, 2018. — 318 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0705-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/922734
4. Кузин А.В., Кузин Д.А. Компьютерные сети: учебное пособие / А.В. Кузин, Д.А. Кузин. — 4-е изд., перераб. и доп. — Москва: ФОРУМ: ИНФРА-М, 2019. -192 с.: ил. – (Профессиональное образование).
5. Монк С., Шерц П. Электроника. Теория и практика. 4-е издание: пер. с англ. — БХВ-Петербург, 2018—1168 с. — ISBN 978-5-9775-3847-3
6. Пальмов, С. В. Методы и средства моделирования программного обеспечения: конспект лекций / С. В. Пальмов. — Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. — 105 с. — ISBN 2227-8397. — Текст: электронный // Электронно-библиотечная система IPR BOOKS: [сайт]. — URL: http://www.iprbookshop.ru/71855.html
7. Статистика России и мира – информация и показатели. [Электронный ресурс] – URL: https://rosinfostat.ru/potreblenie-elektroenergii/

ПРОЕКТИРОВАНИЕ СИСТЕМЫ ФИКСАЦИИ И АНАЛИЗА ПОЛУЧАЕМЫХ ЗАЯВОК ИНТЕРНЕТ-ПРОВАЙДЕРА

Магомедова Мадина Алиевна, студентка четвертого курса
Магомедова Марина Алиевна, студентка четвертого курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В современном мире информация рассматривается как один из основных ресурсов развития общества, а информационные системы и технологии используются в производственной, управленческой, финансовой и многих других деятельностях.

Отыскание рациональных решений в любой сфере требует больших объемов информации, что подчас невозможно без привлечения специальных технологических средств.

Внедрение информационных технологий, современных средств переработки и передачи информации в различные сферы деятельности послужило началом информации, которая является реакцией общества на потребность в существенном увеличении производительности труда в различных сферах деятельности человека, а также ее автоматизация и учета, что позволяет облегчить работу ручного труда. Для успешного развития бизнеса необходимо решить проблемы учета приема и выполнения заявок клиентов.

Целью данной научно-исследовательской работы является разработка информационной системы фиксации и анализа получаемых заявок интернет- провайдера.

Предметной областью научно-исследовательской работы является интернет-провайдер, в основной вид деятельности которого входит предоставление пользователям доступа к сети Интернет, а также прочие услуги, связанные с доступом к интернету.

В число предоставляемых Интернет-провайдером услуг могут входить:

- доступ в Интернет по коммутируемым и выделенным каналам;
- беспроводной доступ в интернет;
- выделение дискового пространства для хранения и обеспечения работы сайтов (хостинг);
- поддержка работы почтовых ящиков или виртуального почтового сервера;
- аренда выделенных и виртуальных серверов;
- резервирование данных;
- и другие.

Как правило, огромное число поступающих заявок вызывает большую нагрузку на диспетчеров. Для данного предприятия необходимо внедрение информационной системы фиксации и анализа заявок, что и является актуальностью работы.

На рисунке 1 представлена диаграмма потоков данных, которая показывает движение различных потоков данных в рассматриваемой предметной области.

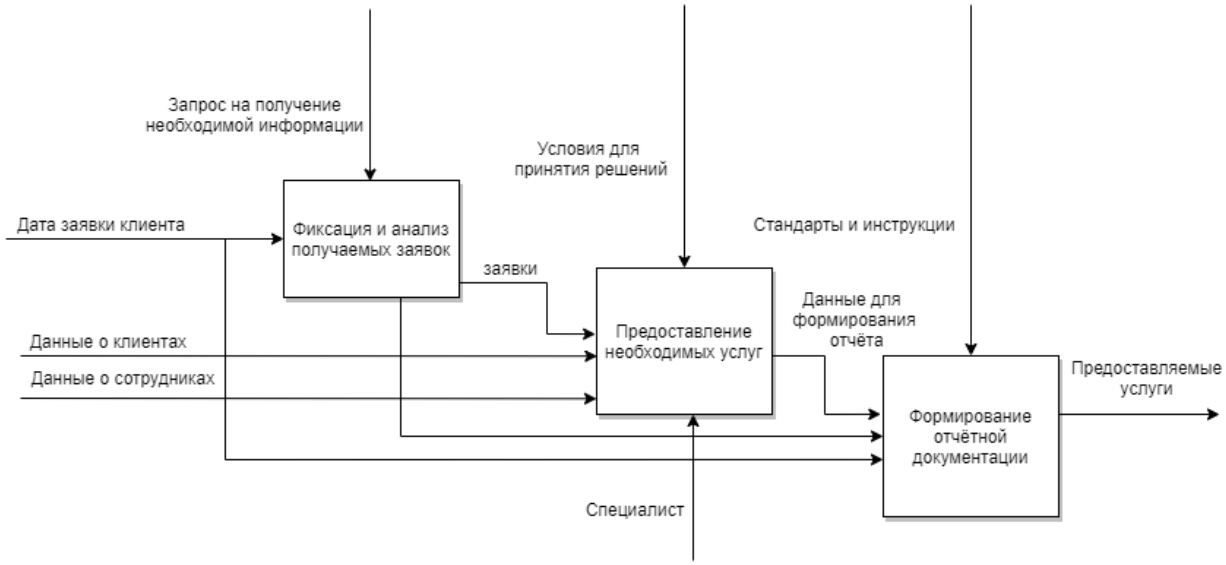


Рисунок 1 – Диаграмма потоков данных

Для хранения информации в СУБД MS SQL Server была разработана базы данных. Графическое представление созданной базы данных, представляется с помощью схемы данных. Схема данных представляет набор схем всех таблиц созданной базы данных, которая представлена на рисунке 2.

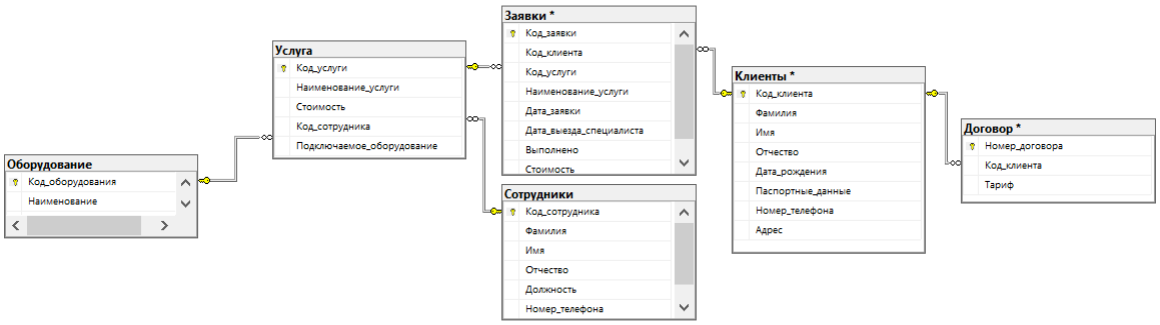


Рисунок 2 – Схема данных

Приложение было разработано в среде Visual Studio с использованием языка программирования C#.

Администратор базы данных (DBA) — лицо, отвечающее за выработку требований к базе данных, её проектирование, реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей БД и защиту от несанкционированного доступа. Не менее важной функцией администратора БД является поддержка целостности базы данных.

По мере того как деятельность организаций всё больше зависит от компьютерных информационных технологий, проблемы защиты баз данных становятся всё более актуальными. Угрозы потери конфиденциальной информации стали обычным явлением в современном компьютерном мире. Если в системе защиты есть недостатки, то данным может быть нанесён ущерб, который может быть выражен в: нарушении целостности данных, потере важной информации, попадании важных данных посторонним лицам и так далее.

Чтобы обеспечить защиту данных в компьютерных системах необходимо определить перечень мер, обеспечивающих защиту. Основными методами защиты баз данных являются защита паролем, шифрование, разграничение прав доступа.

Основным средством защиты информации является защита паролем. Защита паролем - это простой и эффективный способ защитить вашу базу данных от несанкционированного доступа. Пароли устанавливаются конечными пользователями или администраторами баз данных. Защита информации в информационных сетях стала актуальной с развитием интернета.

Задачи администратора БД:

- проектирование базы данных;
- оптимизация производительности базы данных;
- обеспечение и контроль доступа к базе данных;
- обеспечение безопасности в базе данных;
- резервирование и восстановление базы данных;
- обеспечение целостности баз данных.

Результатом научно-исследовательской работы является разработанная ИС фиксации и анализа получаемых заявок интернет – провайдера.

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие/ А.В Васильков, И.А. Васильков. - М: ФОРУМ: ИНФА-М,2017. - 384 с.

2. Конова Е.А., Поллак Г.А. Язык С++: Учебное пособие. - 4-е изд, стер. - СПб.: Издательство «Лань», 2019. - 384 с.

3. Немцова Т.И. Программирование на языке высокого уровня программирование на языке С++: учебное пособие.

4. Сайт для программистов C#: [Электронный ресурс]. - http://www.programmerlib.ru/csharp.php

5. Гагарина Л.Г. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие. -324 с.:ил.

НЕЙРОННЫЕ СЕТИ

Маямсин Сергей Андреевич, ЗКВ 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
«Московский университет Министерства внутренних дел Российской Федерации
имени В.Я. Кикотя», г. Москва

Нейронные сети представляют собой набор алгоритмов, они предназначены для имитации человеческого мозга, то есть предназначены для распознавания образов. Они интерпретируют данные через форму машинного восприятия путем маркировки или кластеризации необработанных входных данных.

Давайте рассмотрим человеческий мозг. Мозг, состоящий из сети нейронов, представляет собой очень сложную структуру. Он способен быстро оценивать и понимать контекст множества различных ситуаций. Компьютеры с трудом реагируют на ситуации подобным образом. Искусственные нейронные сети являются способом преодоления этого ограничения.

Впервые разработанные в 1940-х годах искусственные нейронные сети пытаются имитировать работу мозга. Иногда называемая персептронами, искусственная нейронная сеть представляет собой аппаратную или программную систему. Некоторые сети представляют собой комбинацию этих двух. Состоящая из сети слоев, эта система устроена так, чтобы воспроизводить работу нейронов в мозге.

Сеть состоит из входного слоя, куда вводятся данные, и выходного слоя. Выходной слой — это то место, где представлена обработанная информация. Соединение двух является скрытым слоем или слоями. Скрытые слои состоят из блоков, которые преобразуют входные данные в полезную информацию для представления выходного слоя. Помимо репликации человеческого прогресса в принятии решений искусственные нейронные сети позволяют компьютерам учиться. Их структура также позволяет Энн надежно и быстро идентифицировать паттерны, которые слишком сложны для людей, чтобы их идентифицировать. Искусственные нейронные сети также позволяют быстро классифицировать и кластеризировать большие объемы данных.

Для чего используются искусственные нейронные сети?

Искусственные нейронные сети можно использовать по-разному. Они могут классифицировать информацию, группировать данные или предсказывать результаты. Это можно использовать для самых разных задач. Они включают в себя анализ данных, транскрибирование речи в текст, включение программного обеспечения для распознавания лиц или предсказание погоды. Существует множество типов искусственных нейронных сетей.

Каждый из них имеет свое специфическое назначение. В зависимости от поставленной задачи обработка Энн может быть простой или очень сложной. Самым основным типом искусственной нейронной сети является нейронная сеть прямой связи. Это базовая система, в которой информация может перемещаться только в одном направлении-от входа к выходу.

Различные типы нейронных сетей

Наиболее часто используемым типом искусственной нейронной сети является рекуррентная нейронная сеть. В этой системе данные могут течь в нескольких направлениях. В результате эти сети обладают большей способностью к обучению. Следовательно, они используются для выполнения сложных задач, таких как распознавание языка. Другие типы искусственных нейронных сетей включают сверточные нейронные сети, сети Хопфилда и машинные сети Больцмана. Каждая сеть способна выполнять определенную задачу. Данные, которые вы хотите ввести, и приложение, которое вы имеете в виду, влияют на то, какую систему вы используете. Сложные задачи, такие как распознавание голоса, могут потребовать более одного типа ANN.

Для чего используются искусственные нейронные сети?

Искусственные нейронные сети можно использовать по-разному. Они могут классифицировать информацию, группировать данные или предсказывать результаты. Энн можно использовать для самых разных задач. Они включают в себя анализ данных, транскрибирование речи в текст, включение программного обеспечения для распознавания лиц или предсказание погоды. Существует множество типов искусственных нейронных сетей.

Каждый из них имеет свое специфическое назначение. В зависимости от поставленной задачи обработка Энн может быть простой или очень сложной. Самым основным типом искусственной нейронной сети является нейронная сеть прямой связи. Это базовая система, в которой информация может перемещаться только в одном направлении-от входа к выходу.

Различные типы нейронных сетей

Наиболее часто используемым типом искусственной нейронной сети является рекуррентная нейронная сеть. В этой системе данные могут течь в нескольких направлениях. В результате эти сети обладают большей способностью к обучению. Следовательно, они используются для выполнения сложных задач, таких как распознавание языка. Другие типы искусственных нейронных сетей включают сверточные нейронные сети, сети Хопфилда и машинные сети Больцмана. Каждая сеть способна выполнять определенную задачу. Данные, которые вы хотите ввести, и приложение, которое вы имеете в виду, влияют на то, какую систему вы используете. Сложные задачи, такие как распознавание голоса, могут потребовать более одного типа ANN.

Список использованных источников

1. Галушкин, А.И. Нейронные сети: основы теории. / А.И. Галушкин. - М.: РиС, 2015. - 496 с.
2. Редько, В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики / В.Г. Редько. - М.: Ленанд, 2019. - 224 с.

ЗАЩИТА ОТ АТАК НА DHCP-СЕРВЕР

Михайлов Александр Сергеевич, студент 3 курса
Научный руководитель Поликарпов Евгений Сергеевич, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
«Московский университет Министерства внутренних дел Российской Федерации
имени В.Я. Кикотя», г. Москва

Общая характеристика службы DHCP

DHCP (Dynamic Host Configuration Protocol – протокол динамической конфигурации узла) – это протокол, который позволяет устройствам в сети автоматически получать сетевые параметры (в том числе и IP-адрес).

Клиент, настроенный на автоматическое получение IP-адреса отправляет широковещательные адреса сетевого (IP-адрес 255.255.255.255) и канального (MAC-адрес – FF:FF:FF:FF:FF:FF) уровней для обнаружения DHCP-серверов. Данный пакет получают все устройства в сети, но отвечает на него только DHCP-сервер. До получения IP-адреса от одного из возможных DHCP-серверов в поле адреса источника IP-пакета указывается IP-адрес 0.0.0.0, т.к. клиент еще не получил данный параметр. В поле источника сообщения на канальном уровне указывается MAC-адрес клиента. Такое сообщение называется «DHCPDISCOVER».

Если вдруг на данное сообщение клиента не ответил ни один DHCP-сервер в течение одной секунды, то клиент повторно отправляет запросы еще пять раз (интервал между запросами составляет приблизительно 30 сек). В случае, если ответ от сервера так и не получен, то клиент получает IP-адрес по технологии APIPA (Automatic Private IP Addressing) из диапазона от 169.254.0.1 по 169.254.255.254 с маской подсети 255.255.0.0.

После того, как любой из возможных DHCP-серверов получает широковещательное сообщение, описанное выше, он отправляет на MAC-адрес клиента пул предлагаемых IP-адресов. Данное сообщение, адресованное от сервера к клиенту, называется «DHCPOFFER». На время предложения данные IP-адреса резервируются DHCP-сервером и не предлагаются другим клиентам. Данные действия проделывают все DHCP-сервера, получившие широковещательное сообщение.

Предположим, что клиент получил сообщение «DHCPOFFER» от одного из DHCP-серверов. Тогда клиент отправляет широковещательное сообщение «DHCPREQUEST», в котором содержится IP-адрес сервера, выдавшего предложение. Такое широковещательное сообщение информирует другие DHCP-серверы о том, что клиент уже принял предложение от одного из серверов. В таком случае остальные DHCP-серверы освобождают зарезервированные IP-адреса и в дальнейшем они могут быть предложены другим клиентам.

После получения сервером сообщения «DHCPREQUEST» он вносит выбранный клиентом IP-адрес в определенное поле сообщения «DHCPACK». После получения подтверждения клиент полностью инициализирует протокол TCP/IP на своем сетевом интерфейсе.

Виды атак на DHCP-сервер

Существует два основных вида атак на DHCP-сервер: DHCP Starvation и Rogue DHCP. Принцип работы DHCP Starvation в следующем: генерируется большое количество сообщений типа «DHCPDISCOVER» с запросом аренды IP-адреса на широковещательные адреса сетевого и канального уровней, на порт назначения – 67, т.е. на DHCP-сервер. При этом MAC-адрес источника каждый раз изменяется на новый. Соответственно, DHCP-сервер, получая такие сообщения, резервирует IP-адреса из пула, что и приводит к отказу в обслуживании легитимных клиентов, желающих арендовать IP-адрес для выхода в сеть.

Rogue – от англ. мошенник. Атака Rogue DHCP является видом атаки типа Man in the Middle (человек посредине). Суть этой атаки заключается в развертывании поддельного DHCP-сервера, который в свою очередь будет предоставлять аренду клиентам поддельные сетевые параметры, а именно – адрес шлюза. В качестве адреса шлюза выступает IP-адрес

атакующей машины. Таким образом, сетевой трафик, отправляемый клиентами в удаленные сети, будет проходить через шлюз по умолчанию (атакующую машину), что позволит «прослушивать» трафик ничего не подозревающих клиентов.

Защита от атак на DHCP-сервер на примере сетевого оборудования Cisco

Предотвратить атаку типа DHCP Starvation можно с помощью функции безопасности порта коммутатора Cisco. Работа этой функции заключается в ограничении количества допустимых MAC-адресов на определенном порту коммутатора, которым доступ разрешен.

Что касается атаки Rogue DHCP, то предотвратить ее можно также с помощью функции безопасности коммутаторов. Для этого коммутатор настраивается функцией DHCP Snooping, с помощью которой он отбрасывает DHCP-пакет (а именно сообщения, адресованные от сервера клиенту: DHCPOFFER, DHCPACK, DHCPNACK), который пришел на ненадежный порт. Тем самым становится невозможным развертывание поддельного DHCP-сервера, так как коммутатор будет просто отбрасывать его пакеты.

Также, необходимо не забывать о ведении журнала службы DHCP. При расследовании инцидентов источником доказательственной базы могут служить системные события службы DHCP. К примеру, изучив логи DHCP-сервера в сети можно выяснить в какой промежуток времени устройство с определенным физическим адресом владело некоторым арендованным IP-адресом.

Список использованных источников

1. Максимов, Н.В. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - М.: Форум, 2017. - 320 с.
2. Новожилов, Е.О. Компьютерные сети: Учебное пособие / Е.О. Новожилов. - М.: Academia, 2017. - 288 с.
3. Олифер, В. Компьютерные сети. Принципы, технологии, протоколы: Учебник / В. Олифер, Н. Олифер. - СПб.: Питер, 2016. - 176 с.

КОРПОРАТИВНЫЕ МЕССЕНДЖЕРЫ КАК СОВРЕМЕННОЕ СРЕДСТВО КОММУНИКАЦИИ

Морозов Даниил Эдуардович, студент 4-го курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Автоматизация повседневных задач и операций является одним из важнейших процессов любого производственного предприятия, требующий программного обеспечения с мощным функционалом.

Корпоративный мессенджер решает вопрос коммуникации сотрудников внутри компании, а также поддерживает связь с клиентами, подрядчиками и партнерами.

Актуальностью данной работы является исследование функционала корпоративных мессенджеров на предприятии, проектирование ИС для распределения заданий, а также обеспечение коммуникаций сотрудников между собой.

Каждая компания, неважно, работает в ней 10 или 1000 человек, сталкивается с вопросом: «Какой использовать корпоративный мессенджер?» Ведь он в идеале должен объединять все внутренние и внешние коммуникации в одно пространство.

Сегодня рынок корпоративных мессенджеров предлагает десятки вариантов с разным функционалом, интеграцией с другими сервисами и ценовой политикой. Главная особенность – это возможность сэкономить на используемом ПО.

Рассмотрев требования рассматриваемой предметной области был разработан корпоративный мессенджер с необходимым функционалом.

На первом этапе необходимо смоделировать диаграмму потоков входных и выходных данных, чтобы определить основные процессы.

На рисунке 1 представлена модель входной и выходной информации.

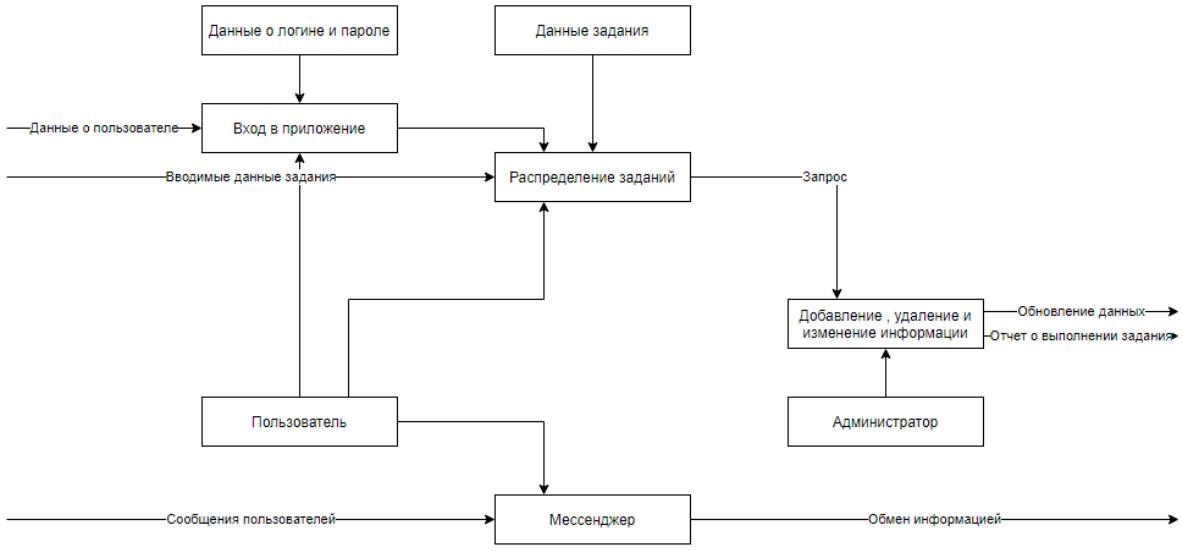


Рисунок 1 – Модель входной и выходной информации

На основе полученных данных можно построить инфологическую модель, которая отображает различимые сущности, находящиеся в определенных связях друг с другом. Цель инфологического моделирования - обеспечение наиболее естественных для человека способов сбора и представления той информации, которую предполагается хранить в создаваемой базе данных. Поэтому инфологическую модель данных пытаются строить по

аналогии с естественным языком (последний не может быть использован в чистом виде из-за сложности компьютерной обработки текстов и неоднозначности любого естественного языка). Основными конструктивными элементами инфологических моделей являются сущности, связи между ними и их свойства (атрибуты).

На рисунке 2 представлена инфологическая модель предметной области.

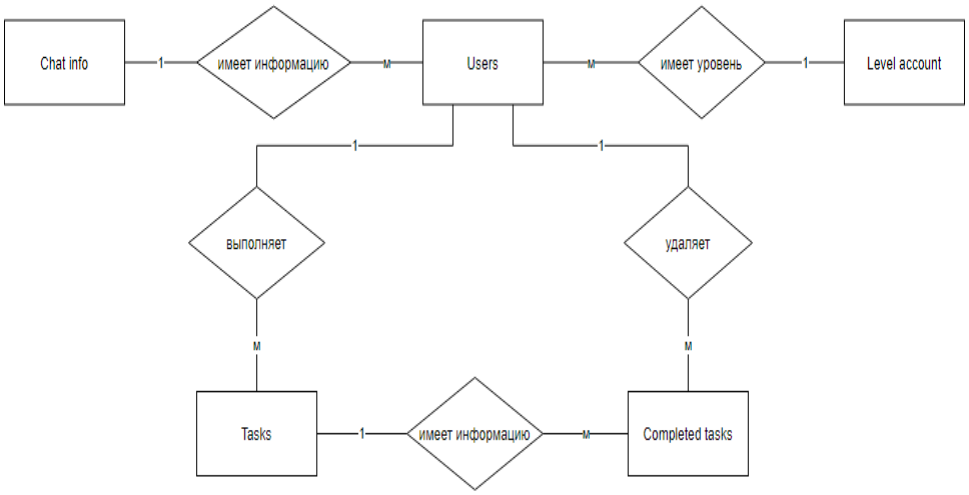


Рисунок 2 - Инфологическая модель предметной области

Для разработки приложения была выбрана СУБД MySQL и среда разработки Visual Studio.

Для визуализации задач были разработаны оконные формы с необходимым набором атрибутов.

Мессенджер предполагает предварительную регистрацию участников или, если пользователь уже был зарегистрирован, просто авторизацию. А сам чат имеет вид общего канала для переписки с возможность посылать личные сообщения конкретному сотруднику организации, также зарегистрированному в мессенджере.

На рисунке 3 представлена главная форма.

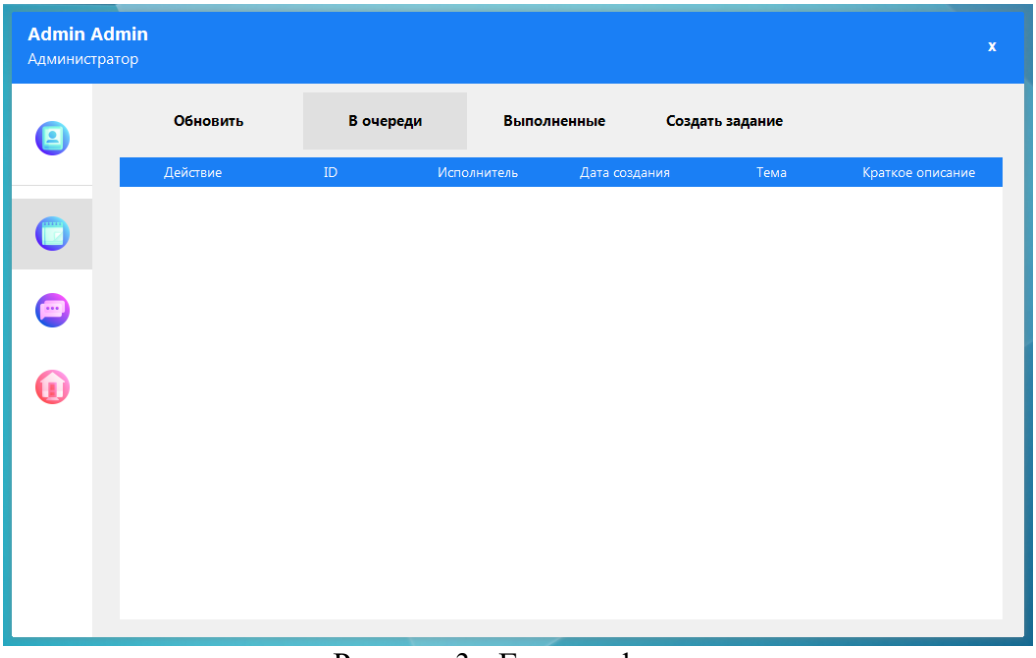


Рисунок 3 - Главная форма

Автоматически при открытии главной формы активной вкладкой является – задачи. На этой вкладке сотрудник может посмотреть все задания, которые в состоянии в очереди или выполнены, а также можно увидеть список пользователей для просмотра информации о них.

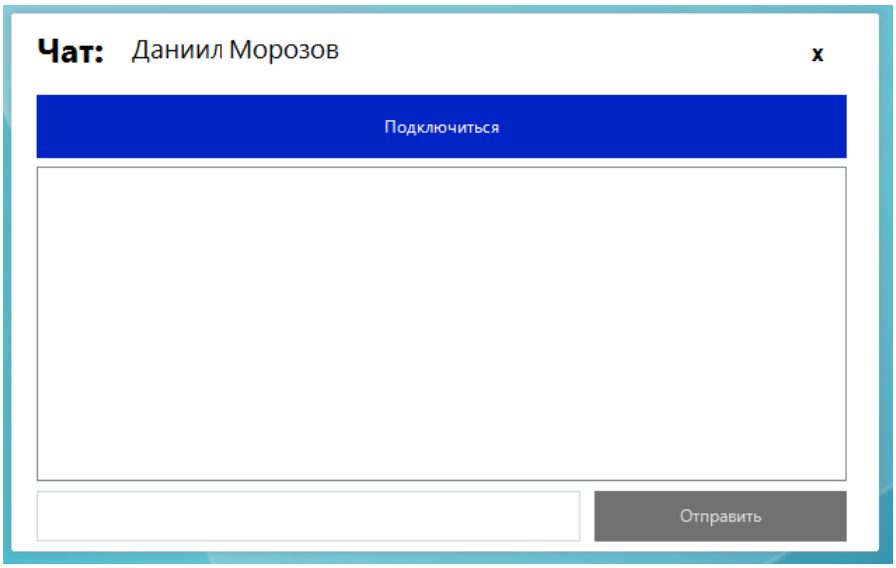


Рисунок 4 - Форма мессенджера

При нажатии на вкладку – мессенджер, появится таблица с выбором пользователя. После выбора пользователя открывается форма мессенджера. При нажатии на вкладку – личный кабинет, появится блок с информацией о пользователе с возможностью ее изменить. На рисунке 5 представлен данный блок.

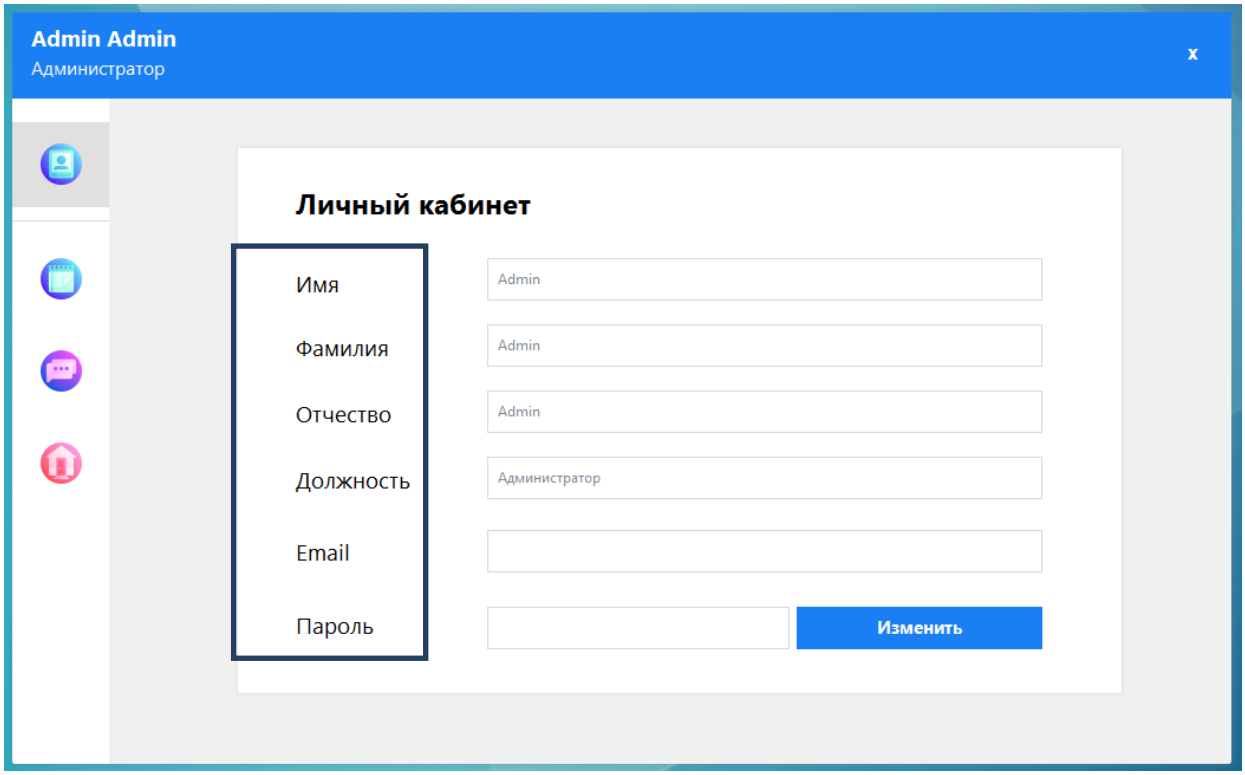


Рисунок 5 - Блок с информацией о пользователе

При нажатии на вкладку – сменить пользователя, выведет с аккаунта и переправит на форму авторизации.

Таким образом, разработанная информационная система представляет собой платформу для мгновенного обмена сообщениями и материалами между сотрудниками предприятия. Помогает бизнесу систематизировать корпоративную коммуникацию и обеспечить максимально защищенное взаимодействие между сотрудниками. Разработка корпоративного мессенджера была построена таким образом, чтобы минимизировать недостатки известных мессенджеров. В разработанном мессенджере вся переписка хранится на сервере организации, к которому нет доступа посторонним лицам извне. Это позволит обеспечить безопасность корпоративной информации, которая может обсуждаться как в личном, так и в общем чате.

Список использованных источников

1. Васильков А.В., Васильков И.А. Безопасность и управление доступом в информационных системах: учебное пособие / А.В. Васильков, И.А. Васильков. – М.: ФОРУМ: ИНФРА-М, 2017. – 368с.
2. Сайт для программистов C#: [Электронный ресурс]. – http://www.programmer-lib.ru/csharp.php
3. Информационный сайт по выбору таск-менеджера - https://coba.tools/compilation/top-7-task-menedzherov
4. Мурадханов, С. Э. Разработка на языке C# приложений с графическим интерфейсом : использование Windows Forms : учебник / С. Э. Мурадханов. - Москва : Изд. Дом НИТУ «МИСиС» - https://znanium.com/catalog/product/1232758

ПРОЕКТИРОВАНИЕ МОДУЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ПОСТРОЕНИЯ ОПТИМАЛЬНОГО МАРШРУТНОГО ПУТИ НА ОСНОВЕ АЛГОРИТМА «ДЕЙКСТРЫ»

Новиков Давид Эдуардович, студент 3 курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Нахождение кратчайшего пути – необходимо и используется практически везде, начиная от нахождения оптимального маршрута между двумя объектами, например на местности или в программе, о нахождении оптимального маршрута при перевозках, Автопилота и т.п.

Актуальностью темы является широкое применение различных методов и теорий о нахождении кратчайших путей в цепи.

В современном мире предпринимаются и создаются все необходимые условия, для комфортной, удобной и как можно менее энергозатратной деятельности человека.

Создаются различные технические устройства, которые помогают минимизировать участие человека практически во всех отраслях производства. Однако, очень большое количество разнообразных задач невозможно выполнить без прямого либо косвенного вмешательства человека. Эта проблема обусловлена недостаточным уровнем развития технологий на данном этапе существования человечества. Одной из задач, требующих непосредственно вмешательства человека, является доставка товаров.

Практически все задачи, связанные с доставкой и распределением товаров, являются задачами такого подраздела экономики, как логистика. Именно эта отрасль занимается изучением способов построения как можно более коротких маршрутов для оптимизации работы по распределению, перевозке и доставке товаров.

Целью создания программного обеспечения является автоматизированный свод, учет и нахождение минимальных затрат времени на перевозку товара. Готовое ПО может использовать любая компания, занимающаяся поставками товаров.

Моделирование основных и вспомогательных процессов предметной области

Диаграмма сценария работы предприятия, занимающегося поставкой товара в рассматриваемой предметной области представлена на Рисунке 1.

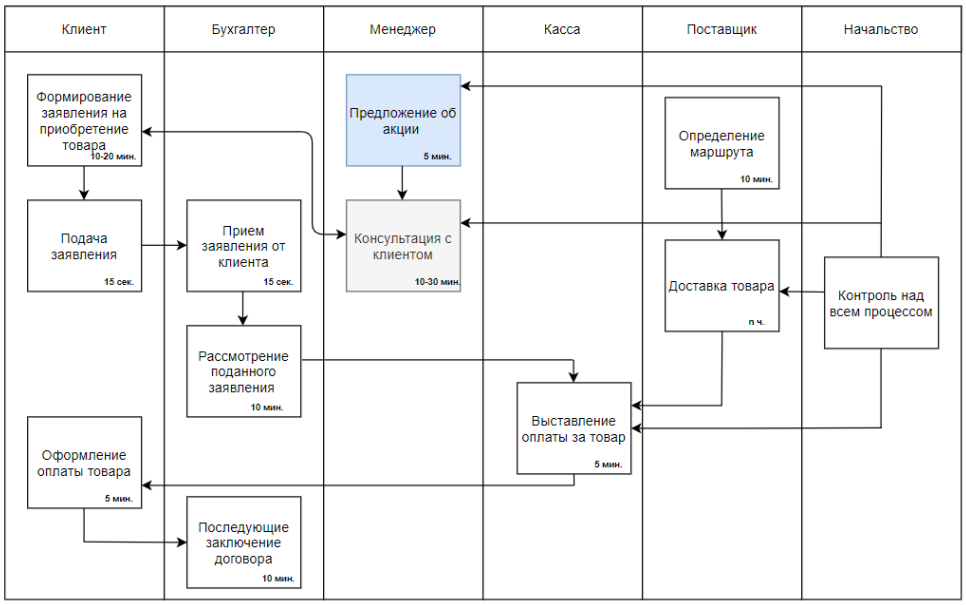


Рисунок 1 – Диаграмма сценария работы предприятия, занимающегося поставкой товара

Клиент подаёт заявку, которая обрабатывается через менеджера к бухгалтеру, после чего происходит расчёт этого товара и выставление счёта. Менеджер ведёт отчётность по заказам.

Клиент оплачивает, выставленный бухгалтером счёт. Для каждой заявки бухгалтер контролирует платёжный счёт.

Поставщик определяет маршрут и решает вопрос с доставкой клиенту. Начальство контролирует все процессы.

Диаграмма конечных автоматов рассматриваемой предметной области представлена на Рисунке 2.

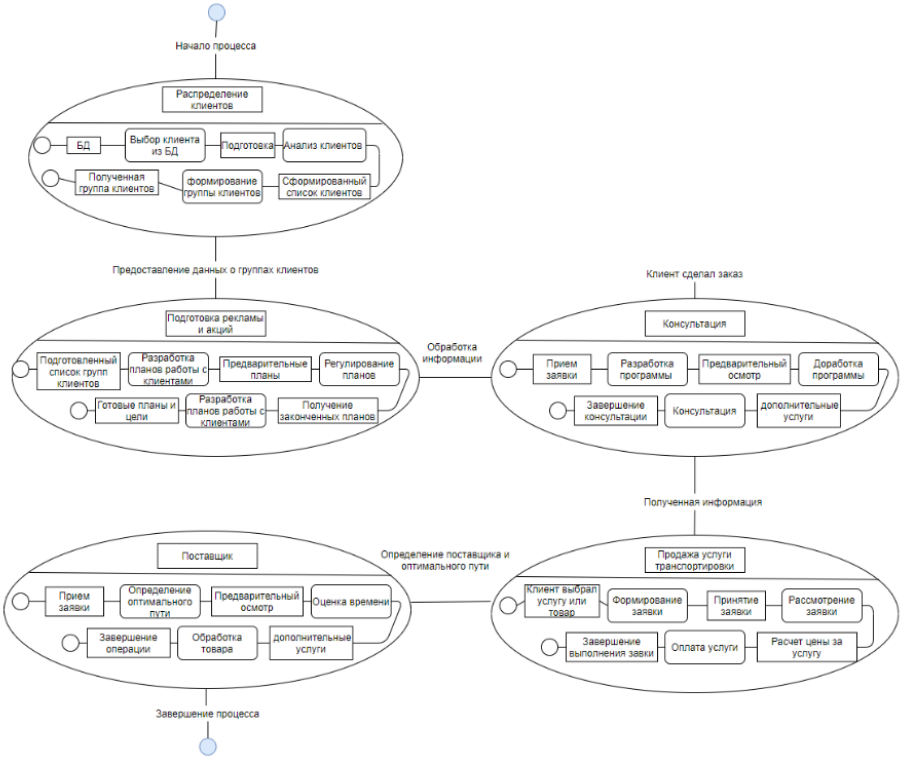


Рисунок 2 – Диаграмма конечных автоматов

Диаграмма конечных автоматов описывает все возможные состояния одного экземпляра определенного класса и возможные последовательности его переходов из одного состояния в другое.

Получив модели предметной области, описывающие основные и вспомогательные процессы, можно определить входные и выходные данные. На рисунке 3 изображена диаграмма входных/выходных данных.

Рисунок 3 – Диаграмма потоков входных/выходных данных

Окно авторизации/регистрации и главное форма разрабатываемого приложения изображено на рисунке 4-5соответственно.

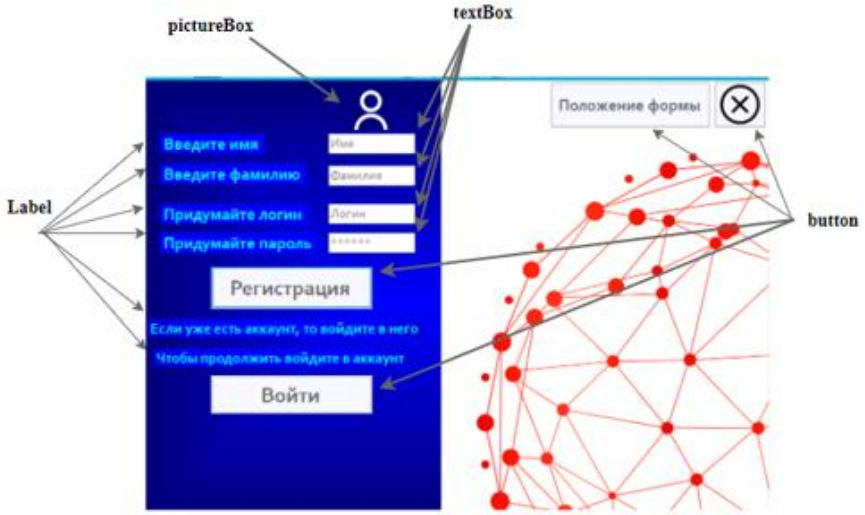


Рисунок 4 – Окно авторизации/регистрации

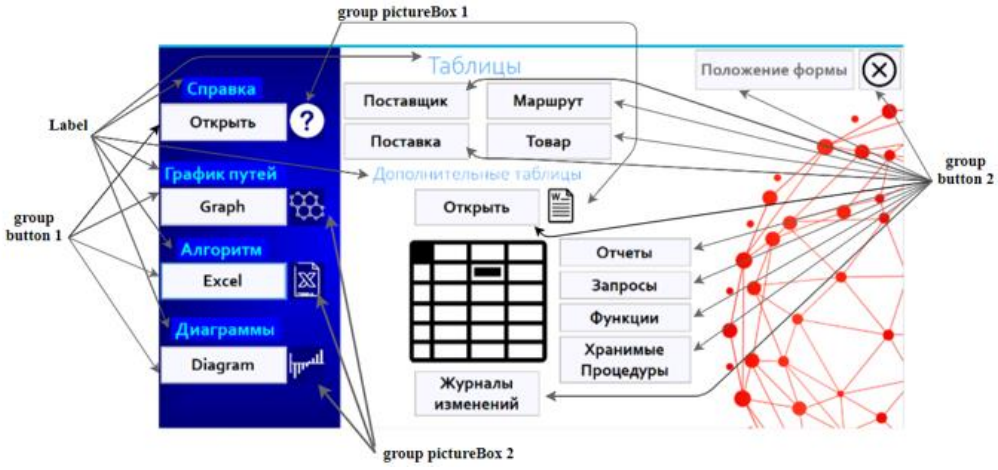


Рисунок 5 – Главная форма

Окно построения графа согласно алгоритму «Дейкстры» представлен на рисунке 6.

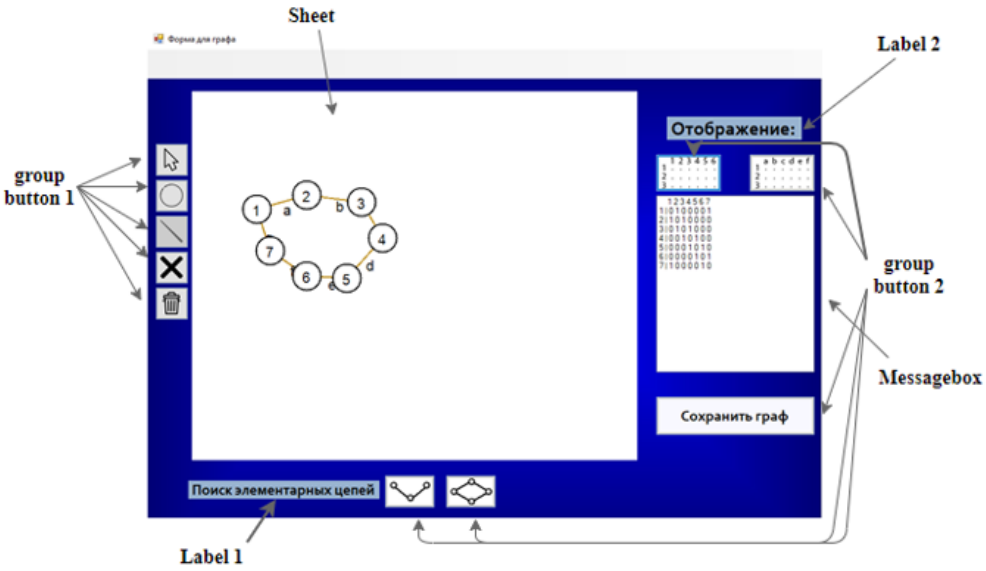


Рисунок 6 – Окно построения графа

Разработанное приложение позволит решить следующие задачи:

- спроектировать возможность построения графа для нахождения оптимального пути;
- спроектировать возможность определения матрицы инцидентности ориентированного графа;
- реализовать возможность определения матрицы смежности ориентированного графа;
- осуществить возможность нахождения оптимального маршрута на основе алгоритма «Дейкстры»;
- реализовать разграничение прав доступа пользователей к приложению в зависимости от представленных им прав доступа к информации;
- реализовать контроль в системе накопления и хранения статистики о работе предметной области для подготовки сводной отчетности, а также анализа динамики деятельности предметной области.

Список использованных источников

1. Гвоздева, В. А. Основы построения автоматизированных информационных систем: учебник / В.А. Гвоздева, И.Ю. Лаврентьева. – Москва: ИД «ФОРУМ»: ИНФРА–М, 2018. – 318 с. – (Среднее профессиональное образование). – ISBN 978-5-8199-0705-4. – Текст: электронный. – URL: https://znanium.com/catalog/product/922734
2. Пальмов, С. В. Методы и средства моделирования программного обеспечения: конспект лекций / С. В. Пальмов. – Самара: Поволжский государственный университет телекоммуникаций и информатики, 2016. – 105 с. – ISBN 2227-8397. – Текст: электронный // Электронно–библиотечная система IPR BOOKS: [сайт]. – URL: http://www.iprbookshop.ru/71855.html
3. ЭдсгерДейкстра: в поисках «кратчайшего пути» к осознанному программированию [Электронный ресурс]: https://habr.com/ru/post/303712/
4. Алгоритм «Дейкстры» нахождения кратчайшего пути [Электронный ресурс]: https://prog-cpp.ru/deikstra/
5. Объяснение Графов [Электронный ресурс]: https://prog-cpp.ru/data-graph/

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ WEB-ПРОГРАММИРОВАНИЯ ДЛЯ АВТОМАТИЗАЦИИ БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЯ

Саплин Никита Вячеславович, студент второго курса
Научный руководитель Семенов Андрей Владимирович, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

Аннотация: В данной статье рассматривается проблема использования организацией малодейственных методов распространения информации о своей деятельности. Газетные публикации и справочники могут размещать не полную информацию об организации, в результате чего отсутствует возможность оперативного изменения информации, так как выпуск печатных изданий ведется крупными тиражами и занимает продолжительные интервалы времени.

Для успешного существования компании в условиях современной конкуренции клиентам нужно иметь полное представление о предоставляемых услугах, а также их свойствах, цене и т.д. Для того чтобы получить ответы на все интересующие клиента вопросы об оказываемых услугах или их цене, клиент обращается в организацию по телефону, при этом увеличивается количество и продолжительность телефонных звонков, тем самым, нагружая работников организации.

Разработка веб-сайта для организации ООО «Скоростной трамвай» позволит устранить имеющиеся сейчас недостатки в существующей системе распространения информации об услугах, предоставляемых организацией, и выведет на новый уровень эффективность привлечения новых клиентов. Суть состоит в том, чтобы заинтересовать потенциального клиента, донести положительную информацию об общественном электротранспорте.

Созданный сайт будет являться источником по сбору первичной информации и предназначен для отображения пользователям этой информации в конечном виде.

Ключевые слова: web-платформа, база данных, общественный электротранспорт.

Актуальностью данной работы является организация работы трамвайного депо.

Целью работы является разработка навигационной web-платформы для организации работы трамвайного депо.

Разработанный web-сайт должен соответствовать следующим требованиям:

– иметь понятный интерфейс, как для специалистов компании, так и для потенциальных клиентов;

– предоставлять необходимую информацию об организации на веб-сайте;

– предоставлять возможность администрирования сайта сотрудниками компании – что снизит расходы на содержание информационного ресурса и уменьшит время простоя в случае сбоев;

– иметь возможность легкого изменения - важно, чтобы веб-сайт был динамичным, постоянно развивался и совершенствовался для увеличения эффективности от его работы, при этом с минимальными денежными затратами.

Входная информация – информация, которая поступает из других источников или систем, либо вводится вручную. Входной информацией данной предметной области являются:

- История организации.
- Руководство организации.
- Структура организации.
- Информация о маршрутах.
- Информация о расписаниях.
- Информация о стоимости проезда.

Выходная информация – информация, которая является результатом работы. Выходной информацией данной предметной области являются:

- Страницы с информацией об организации.
- Страницы с информацией для пассажиров.
- Страницы с информацией о вакансиях.

В качестве управляющих механизмов данной предметной области выступают:

- Устав организации.

В качестве механизмов, выполняющих бизнес-процессы данной предметной области, выступают:

- Администратор.
- База данных.

Логическая структура веб-сайта – это система организации ссылок между страницами веб-сайта. Структура веб-сайта определяется на первых этапах создания проекта, до начала разработки дизайна [7].

На рисунке 1 представлена логическая структура сайта, относящаяся к древовидному типу.

Рисунок 1 – Логическая структура сайта

Физическая структура сайта – подразумевает алгоритм размещения физических файлов по поддиректориям папки, в которой хранится разработанный сайт [6].

На рисунке 2 представлена физическая структура сайта.

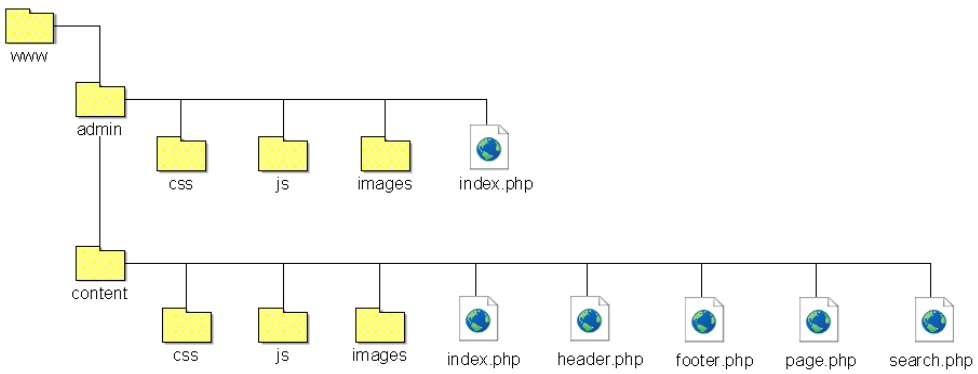


Рисунок 2 – Физическая структура сайта

Web-страница представляет собой набор прямоугольных блоков, которые выкладываются в определенном порядке. При этом, как правило, данные располагаются по колонкам, поэтому при верстке применяют термин одно-, двух-, трехколонный макет.

Компоновка страниц сайта должна обеспечивать автоматическое масштабирование страниц в зависимости от ширины рабочего поля браузера пользователя. Минимальный размер (ширина) рабочего поля браузера, при котором необходимо обеспечить полноценное отображение страниц (без полосы горизонтальной прокрутки), составляет 1024 пиксела [6].

На страницах данного сайта используются следующие элементы:

- Header (шапка сайта) – это блок в верхней части страницы. Используется для размещения логотипа, названия организации, навигационного меню, формы поиска и другой наиболее важной информации.
- Nav (навигационное меню) – это блок который, как правило, находится в шапке сайта. Содержит сгруппированный набор ссылок с названиями разделов, облегчающими переход на другие страницы.
- Footer (подвал сайта) – блок в нижней части страницы. Используется для вывода полезной, но не первостепенной информации. Подвал может содержать: копирайт, контактную информацию, данные об авторе, дополнительные ссылки и т.д.
- Sidebar (боковая панель) – это блок который, как правило, находится с правой стороны страницы. Боковая панель может содержать: дополнительное навигационное меню, различные информационные блоки и функциональные элементы (форму поиска, корзину и т.д.).

Список использованных источников

6. Васильков А. В., Васильков И. А. Безопасность и управление доступом в информационных системах: учебное пособие / А. В. Васильков, И. А. Васильков – М.: ФОРУМ: ИНФРА-М, 2017. – 368 с.

7. Дунаев В. В. Сценарии для Web-сайта PHP и JavaScript. – 2-е изд. перераб. и доп. – СПБ.: БХВ-Петербург, 2017. – 576 с.: ил.

8. Колисниченко Д.А., PHP и MySQL. Разработка веб-приложений / Д.А. Колесниченко. - М., 201. – 592 с.

9. Самоучитель по HTML: [Электронный ресурс]. - http://htmlbook.ru/

10. Форум разработчиков и пользователей SQL: [Электронный ресурс].- https://www.sql.ru/

11. Википедия – свободная энциклопедия: [Электронный ресурс]. - https://ru.wikipedia.org/

12. Учебное пособие по PHP: [Электронный ресурс]. - https://htmlacademy.ru/tutorial/php

13. Сайт о WordPress: [Электронный ресурс]. - https://wp-kama.ru/

ВИРУСЫ И ВРЕДОНОСНЫЕ ПРОГРАММЫ, РАСПРОСТРАНЯЮЩИЕСЯ ПОСРЕДСТВОМ ЗАРАЖЕННЫХ ФАЙЛОВ НА ФАЙЛООБМЕННИКАХ

Сахнов Илья Юрьевич курсант 1 курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры ИБ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Бесспорно, определенное количество вредоносных программ распространяется через такие системы обмена файлами, как торренты и одноранговые сети. Неудивительно, что 48% участников опроса считают, что данный способ является основным в распространении вредоносного ПО. Наверняка тот или другой пользователь уже хотя бы раз заражал свои компьютер вирусом после посещения подобных сайтов. Однако данный тезис также ложен и является мифом, поскольку большинство вредоносных программ распространяется через вредоносные Web-сайты.

Вирусы получили свое название за способность “заражать” множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например USB-накопителях или на дискетах. По данным Национального института стандартов и технологий, первый компьютерный вирус под названием “Brain” был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты.

В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельца. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы и процесс начинается снова.

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

Севастьянов Даниил Сергеевич, курсант 2-го курса
Блохин Егор Владимирович курсант 2-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры ИБ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Большая часть информационных массивов, принадлежащих государственным учреждениям и коммерческим предприятиям, имеет самостоятельную ценность и является добычей для потенциальных похитителей, которыми могут быть и хакеры, и внутренние пользователи.

Для защиты информации от утечек разработаны сложные программные продукты, позволяющие определить проникновение неавторизованного пользователя или вируса-похитителя информации в сеть и блокировать его.

Существуют специальные стандарты защиты информации, но даже они не всегда могут уберечь сети от взлома и хищения данных. Особенно уязвимы компьютеры и мобильные устройства частных пользователей, использующих только антивирусы.

От хищения информации с помощью закладных устройств, перехватывающих электромагнитные излучения, необходимо бороться при помощи технических средств.

Защита информации в телекоммуникационных сетях является одним из ключевых направлений деятельности любой организации.

Средства и методы защиты информации в телекоммуникационных сетях

1. Антивирусная защита рабочих станций,
2. Межсетевой экран или система обнаружения атак.
3. Программно-аппаратное средство формирования защищенных корпоративных сетей.
4. Аппаратные средства аутентификации пользователей.
5. Средства защиты от несанкционированного доступа.
6. Криптографические средства.
7. Организация разграничения доступа пользователей к конфиденциальным данным с помощью штатных механизмов защиты информации.
8. Организация разграничения доступа к операционным системам, прикладным программам, маршрутизаторам и т. п.
9. Программные криптографические средства и средства создания электронной цифровой подписи для обмена конфиденциальными данными через открытые каналы связи.
10. Средства "прозрачного" шифрования логических дисков пользователей.
11. Средства уничтожения неиспользуемых конфиденциальных данных.

В зависимости от цели защиты сведений, ее обладателя и ценности сведений применяются различные защитные меры или их комплексы. В широком смысле их делят на организационные и технические.

Организационные

Организационные средства чаще всего направлены на контроль поведения пользователей, исключая риски отправки служебной или конфиденциальной информации по незащищенным каналам. Иногда это необходимо, так как даже IT-специалисты пользуются частными Wi-Fi-сетями для отправки сообщений, содержащих ценные сведения. Разработка политик безопасности, информирование пользователей об угрозах и уязвимостях должны стать для компании первоочередными организационными мероприятиями, призванными обеспечить безопасность данных.

Разграничение доступа к информации пользователей несмотря на то, что для него требуются аппаратные средства, также относится к организационным мерам. Так, в некоторых корпорациях для пользователей полностью отсутствует возможность выхода в Интернет с рабочих станций, что устраняет опасность утечки с этих ПК по внешним каналам.

Технические

Применяемые в целях обеспечения безопасности корпоративных файлов технические меры доступны большинству квалифицированных IT-специалистов. Выбор зависит от конкретных целей. Среди таких мер:

- криптографическая защита электронных документов;
- подтверждение авторства документа с помощью усиленной электронной подписи (ст. 5 Закона об ЭП), такой тип подписи применяется для наиболее важных документов, например, для заверения постановлений органов власти;
- контроль за целостностью документов;
- идентификация документов, например, их нумерация;
- защищенная передача данных с использованием идентификаторов PHP. Это дает возможность пользователю не авторизовываться каждый раз, переходя на новую страницу, и обеспечивает безопасность данных;
- установка программных решений, которые перехватывают трафик инсайдеров, передаваемый по конфиденциальным каналам связи, и расшифровывают его путем подмены сертификатов. Такие решения стали обычными в российской корпоративной практике;
- динамическая аутентификация пользователей. Примером этой технологии является SMS-рассылка одноразовых паролей;
- использование постоянно меняющихся ключей для шифрования текстов;
- обеспечение сохранности секретных ключей;
- применение электронного сертификата. Электронный сертификат подтверждает принадлежность ключа владельцу, используется при создании ЭЦП;
- создание защищенного соединения. Например, по такому каналу данные из 1С с рабочей станции пользователя могут попадать в «облако».

. Организационные меры не в состоянии предотвратить в полной мере попытки несанкционированного доступа, поскольку они распространяются исключительно на масштабы организации, не охватывая каналы связи, и не предполагают применения технических средств борьбы с угрозами перехвата информационных сообщений. В связи с этим наряду с применением разных приоритетных режимов и систем разграничения доступа разработчики информационных систем уделяют внимание различным криптографическим методам обработки информации.

Антивирусы для защиты рабочих станций и файловых серверов

- Symantec Endpoint Protection Small Business Edition

Продукт Symantec Endpoint Protection Small Business Edition обеспечивает защиту серверов, портативных компьютеров и настольных компьютеров от вирусов, программ-шпионов и другого вредоносного кода с помощью одного интегрированного продукта.

- Kaspersky Small Office Security

Kaspersky Small Office Security — это инновационные технологии защиты мирового класса в сочетании с простотой установки и настройки и удобством использования.

- Trend Micro Enterprise Security for Endpoints and Mail Servers

Пакет Enterprise Security for Endpoints and Mail Servers упрощает систему и сокращает расходы на ее обслуживание благодаря функциям централизованного управления, поддержке различных платформ и гибким возможностям настройки.

- Trend Micro Enterprise Security for Endpoints (TMES-E)

Защита настольных компьютеров, ноутбуков, серверов, систем хранения данных и смартфонов как внутри, так и вне сети благодаря инновационному сочетанию передовых средств защиты от вредоносных программ с «облачными» системами безопасности на базе платформы Trend Micro Smart Protection Network.

- Trend Micro Enterprise Security for Endpoints Light

Защита настольных компьютеров, ноутбуков, серверов, систем хранения данных и смартфонов как внутри, так и вне сети благодаря инновационному сочетанию передовых средств защиты от вредоносных программ с «облачными» системами безопасности на базе платформы Trend Micro Smart Protection Network.

- Trend Micro Worry-Free Business Security Advanced

Worry-Free Business Security надежнее, так как блокирует вирусы, шпионское ПО, спам и другие угрозы, распространяющиеся через почту, файлы и веб-сайты, до их проникновения в сеть вашей организации.

- Trend Micro Worry-Free Business Security Standard

Worry-Free Business Security надежнее, так как блокирует вирусы, шпионское ПО, спам и другие угрозы, распространяющиеся через почту, файлы и веб-сайты, до их проникновения в сеть вашей организации.

- Panda Security for Commandline

Panda Security Commandline - это антивирусный движок последнего поколения. Использует самые инновационные технологии для предоставления наилучшей производительности и отличной низкоуровневой интеграции для платформ Linux, Windows 32-bit и MS-DOS.

Криптографические средства

Криптографические средства защиты данных отличаются различной степенью сложности, в России их сертификацией занимаются такие ведомства, как ФСБ и ФСТЭК РФ.

Испытанный метод защиты информации от несанкционированного доступа - шифрование (криптография). Шифрованием (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст - ciphertext) или зашифрованных данных - в открытые по определенным правилам с применением определенных правил, содержащихся в ключах (шифре).

Известные криптографические методы защиты информации можно разбить на два класса:

1) обработка информации путем замены и перемещения букв, при котором объем данных не меняется (шифрование);

2) сжатие информации с помощью замены отдельных сочетаний букв, слов или фраз (кодирование).

К алгоритмам шифрования предъявляются определенные требования:

• высокий уровень защиты данных против дешифрования и возможной модификации;

• защищенность информации должна основываться только на знании ключа и не зависеть от того, известен алгоритм или нет (правило Керкгоффса);

(Правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей. Широко применяется в криптографии.)

Криптопровайдер

В тех случаях, когда политики безопасности данных допускают возможности использования различных программных средств для шифрования, некоторые компании прибегают к услугам криптопровайдеров. Под этим термином понимается независимый модуль, который работает в рамках операционной системы и шифрует трафик при помощи CryptoAPI. Криптопровайдер является посредником между операционной системой и всеми

приложениями. В России есть ГОСТы, устанавливающие требования к этому способу защиты информации.

Используемые методы шифрования информации не обеспечивают передачи данных в виде документа определенного типа, имеющего конкретное расположение реквизитов в соответствии с установленной формой данного документа. Значимым компонентом для процесса шифрования является лишь содержательная часть документа. В то же время документ целесообразно восстанавливать не только в аспекте содержания, но и сохраняя его форму. Тем самым, наряду со снижением вероятности несанкционированного ознакомления с текстом документа при его передаче по каналам связи, при снижении стоимости шифрования и расшифровки документа будет сохранена не только содержательная часть документа, но и его форма с учетом расположения реквизитов.

Перспективным в плане решения задачи дополнительной защиты документов организации или предприятия, в том числе при передаче их по каналам связи, представляется использование возможностей автоматизированного лексикологического синтеза документов.

Анализ методов шифрования, применяемых в настоящее время, показывает, что, несмотря на достаточно широкое их использование, они не вполне свободны от недостатков и оставляют определенное поле для совершенствования и разработки новых методов защиты информации, передаваемой по каналам связи. Учитывая динамику развития методов управления

Список использованных источников

1. Баранова, Е.К. Информационная безопасность и защита информации: Учебное пособие / Е.К. Баранова, А.В. Бабаш. - М.: Риор, 2018. - 400 с.
2. Глинская, Е.В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие / Е.В. Глинская, Н.В. Чичварин. - М.: Инфра-М, 2018. - 64 с.
3. Ковалев, А.А. Военная безопасность России и ее информационная политика в эпоху цивилизационных конфликтов: Монография / А.А. Ковалев, В.А. Шамахов. - М.: Риор, 2018. - 32 с.

КРИПТОГРАФИЯ

Селицкий Владимир Васильевич, курсант 972 учебного взвода факультета подготовки специалистов в области информационной безопасности

Научный руководитель Казанцев Владимир Иванович, старший преподаватель, доцент

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

С каждым годом компьютерная информация играет все более важную роль в нашей жизни, и все большую актуальность приобретают проблемы ее защиты.

Защита от каждого типа опасности предполагает собственные решения. Впрочем, есть и универсальные подходы, способные обезопасить данные от разных угроз. Одним из них является криптография, то есть шифрование данных.

Изначально криптография использовалась только для безопасного хранения документов. Пользователь зашифровывал их, делая недоступными для злоумышленников. Сегодня область применения криптографии существенно расширилась. Основные изменения связаны с активным использованием асимметричных алгоритмов шифрования (задействованы разные ключи: закрытый и открытый), которые применяются для реализации систем цифровой подписи и сертификатов, безопасной передачи данных по открытым каналам связи и т. д. Симметричное же шифрование (информация зашифровывается и расшифровывается с помощью одного секретного ключа) до сих пор практикуется в основном для защиты сведений от несанкционированного доступа во время хранения. Естественно, современные криптографические системы значительно отличаются от своих предшественников.

Современная криптография и криптосистемы

Симметричные криптосистемы. Современная криптография включает в себя четыре крупных раздела.

В симметричных криптосистемах и для шифрования, и для дешифрования используется один и тот же ключ. Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом, дешифрование — обратный шифрованию процесс. На основе ключа шифрованный текст преобразуется в исходный.

Криптосистемы с открытым ключом. В системах с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения. Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Электронная подпись. Системой электронной подписи называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и подлинность сообщения. Электронная подпись предназначена для защиты электронного документа, передаваемого посредством различных сред или хранящегося в цифровом виде, от подделки и является атрибутом электронного документа. Она получается в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяет идентифицировать владельца сертификата ключа подписи, установить отсутствие искажения информации в электронном документе.

Электронная подпись (ЭП) — это программно-криптографическое средство, которое обеспечивает:

проверку целостности документов;

конфиденциальность документов;

установление лица, отправившего документ.

Электронная подпись используется физическими и юридическими лицами в качестве аналога собственноручной подписи для придания электронному документу юридической силы, равной юридической силе документа на бумажном носителе, подписанного собственноручной подписью правомочного лица и скрепленного печатью.

Электронный документ — это любой документ, созданный при помощи компьютерных технологий и хранящийся на носителях информации, обрабатываемых при помощи компьютерной техники, будь то письмо, контракт или финансовый документ, схема, чертеж, рисунок или фотография.

Использование ЭП позволяет:

значительно сократить время, затрачиваемое на оформление сделки и обмен документацией;

усовершенствовать и удешевить процедуру подготовки, доставки, учета и хранения документов;

гарантировать достоверность документации;

минимизировать риск финансовых потерь за счет повышения конфиденциальности информационного обмена;

построить корпоративную систему обмена документами.

Подделать ЭП невозможно — это требует огромного количества вычислений, которые не могут быть реализованы при современном уровне математики и вычислительной техники за приемлемое время, то есть пока информация, содержащаяся в подписанном документе, сохраняет актуальность. Дополнительная защита от подделки обеспечивается сертификацией Удостоверяющим центром открытого ключа подписи.

С использованием ЭП работа по схеме «разработка проекта в электронном виде - создание бумажной копии для подписи - пересылка бумажной копии с подписью - рассмотрение бумажной копии - перенос ее в электронном виде на компьютер» уходит в прошлое.

ПРИНЦИПЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Симаков Иван Алексеевич, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Информационная безопасность — это практика защиты ваших данных и информации от несанкционированного доступа, и поддержания их конфиденциальности, целостности и доступности в любое время. Она включает в себя методы защиты частной и конфиденциальной информации на печатных или цифровых носителях от несанкционированного изменения, удаления, раскрытия или нарушения.

В целом информационная безопасность защищает ваши данные и информацию от использования субъектами угроз. Она защищает ваши информационные ресурсы при передаче их с одной машины на другую или через физический носитель.

Три основных принципа информационной безопасности

Любая хорошая программа управления информационной безопасностью должна быть разработана для достижения трех принципов информационной безопасности. Вместе они обычно известны как: конфиденциальность, целостность и доступность.

1. Конфиденциальность

Принцип конфиденциальности защищает критически важную информацию от разглашения неуполномоченным лицам, организациям или процессам. Это гарантирует, что конфиденциальная информация остается конфиденциальной, если только кто-то не нуждается в ней для выполнения своих служебных обязанностей.

Вы можете сохранить конфиденциальность информации с помощью паролей, шифрования, многофакторной аутентификации и нескольких других способов. Но сначала необходимо определить, кто и к чему может получить доступ, чтобы ограничить несанкционированный доступ к определенной информации.

2. Целостность

Следующим элементом является целостность информации. Проще говоря, данный принцип определяет полноту и точность информации, гарантируя, что никто не сможет вмешаться в нее намеренно или случайно.

Это гарантирует, что данные и информация являются точными, и вы можете доверять им. Как правило, система информационной безопасности, которая защищает конфиденциальность, также отвечает принципу целостности, поскольку она тщательно проверяет права доступа и гарантирует, что только уполномоченные люди могут видеть информацию.

3. Доступность

Принцип доступности подтверждает, что информация доступна, когда она нужна уполномоченному лицу, организации или процессу. Данный принцип защищает функциональность систем поддержки, делая данные доступными, когда они нужны для принятия решений.

Это включает в себя обеспечение наличия необходимых сетевых и вычислительных ресурсов для облегчения ожидаемого перемещения данных. Кибератаки, такие как атаки типа отказа в обслуживании (DoS), потенциально могут поставить под угрозу доступность

информации. Вы должны поддерживать резервную копию, чтобы доступность информации не пострадала во время инцидентов ИТ-безопасности.

Помимо фундаментальных принципов информационной безопасности, другие принципы регулируют ее меры и практику:

Не отрицание: гарантирует, что автор заявления не может отрицать авторство сообщения (сообщения или подписи), которое они создали.

Аутентичность: проверяет, что пользователи являются теми, за кого они себя выдают, и каждый ввод, который они отправляют адресату, является подлинным.

Подотчетность: она подтверждает, что каждое действие, совершенное субъектом, может быть прослежено до него.

Данные принципы гарантируют, что информация не подвергается изменению, удалению, раскрытию или нарушению, которые может быть вызвано неавторизованными лицами, и подчеркивает надежность информации.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕБ-ПРИЛОЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ OPEN SOURCE РЕШЕНИЙ

Ситников Александр Александрович, курсант 982 взвода, 3 «И» курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры ИБ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

В последнее время в общественную жизнь все больше и больше входят информационные технологии. Они развиваются с невероятной скоростью и влекут за собой череду изменений и совершенствований в различных отраслях современной науки и техники. Информация становится одним из наиболее важных ресурсов как для государства в целом, так и для отдельного человека в частности.

Веб-приложение представляет собой некий алгоритм, зачастую содержащий в основе один или несколько языков программирования, служащий для взаимодействия пользователя, со стороны клиентской части, используя браузер, с удаленным или локальным веб-сервером на базе альтернативных операционных систем Windows или Linux.

Значимость обеспечения безопасности в информационной сфере подчеркнута в «Доктрине информационной безопасности России». Этот документ был издан еще в 2000, но претерпев небольшие изменения был вновь утвержден в декабре 2016 года. Одна из статей несет в себе, на мой взгляд, одну из наиболее важных мыслей всего содержания: «Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.»

Развитие и повсеместное использование информационно-телекоммуникационных технологий, процессы информатизации, а также в реалиях последних событий временные ограничения, направленные на профилактику коронавирусной инфекции, способствуют увеличению количества преступлений в относительно новой сфере преступных посягательств, а именно преступлений в сфере компьютерной информации. Согласно данным ГИАЦ МВД России о состоянии преступности в Российской Федерации за январь-декабрь 2020 года, всего за отчетный период было зарегистрировано 510396 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации.

Инъекции представляют собой класс атак, внедряющий зловредный код в веб-приложение, работающее на стороне сервера или на стороне клиента. В работе рассматриваются 6 основных типов инъекций:

1. HTML инъекции.
2. IFrame инъекции.
3. LDAP инъекции.
4. Инъекции команд ОС.
5. Инъекции PHP кода.
6. SQL инъекции.

Таким образом, в связи с эксплуатацией различных уязвимостей возникает возможность получения несанкционированного доступа к информации, а также ее копирования, модификации, уничтожения. Каждый метод обладает как большим спектром преимуществ, так и не менее большим количеством недостатков. Отметим, что, в большей степени, возможность применения описанных уязвимостей возникает по вине разработчиков и системных администраторов. В свете диверсификации веб-приложений становится критической проблемой обеспечение их безопасности, а также безопасности информации, содержащейся на сервере, но учитывая тенденции развития и уровень подготовки специалистов данной сферы, я считаю, что данная проблема будет постепенно решаться, а

количество раскрытий преступлений, совершенных в сфере компьютерной информации, будет приближено к требуемым нормам.

Список использованных источников

1. Кузнецова, А.В. Искусственный интеллект и информационная безопасность общества / А.В. Кузнецова, С.И. Самыгин, М.В. Радионов. - М.: Русайнс, 2017. - 64 с.
2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.

АНОНИМНОСТЬ В СЕТИ, КАК ПРОБЛЕМА ИНФОРМАЦИОННОГО ОБЩЕСТВА

Скворцов Павел Дмитриевич, курсант 3-го курса
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Пожалуй, многие из Вас задумывались на тему анонимности в сети. Не знаю, устроит ли Вас мой ответ, но я скажу, что и да, и нет. В какой-то мере интернет уже давно является не анонимным, ведь Ваш провайдер обладает полной информацией о нашем трафике. Он видит, какие фильмы мы смотрим, какой тематикой интересуемся, какие сайты посещаем, на каких форумах сидим и так далее. Но то, что он знает о нас абсолютно всё не значит, что нужно надеть шапочку из фольги, а при каждом выходе из дома прятать глаза в пол, не обращая внимания на людей.

Для меня данный вопрос абсолютно не играет никакой роли, я просто принял это как данность и продолжил наслаждаться жизнью, как и раньше. Но здесь речь пойдет не об этом, а о том, как можно обезопасить свои данные в сети.

Идеальная анонимность – это утопия, но несмотря на это, необходимо поддерживать уровень своей анонимности в сети, независимо от ваших целей. Ведь Ваши данные в современном мире являются наиболее ценным товаром, нежели всё остальное. К примеру, зная Ваш интерес к определённой области или товару, будет очень просто продать Вам услугу или какую-либо вещь, которая была Вам просто интересна, но особо-то и не нужна.

Итак, первое, о чём хотелось бы поговорить в рамках данного раздела – это об условных уровнях анонимности. В данной книге мы разделим анонимность на 4 уровня:

1. Базовый уровень защиты
2. Средний уровень защиты
3. Высокий уровень защиты
4. Максимальный уровень защиты

Теперь, давайте поподробнее разберёмся с каждым из этих уровней поподробнее.

Базовый уровень защиты

Данным уровнем необходимо обладать абсолютно каждому пользователю сети, ведь, в первую очередь, Вы обеспечиваете свою безопасность.

Схема базового уровня защиты показана на рисунке 1.

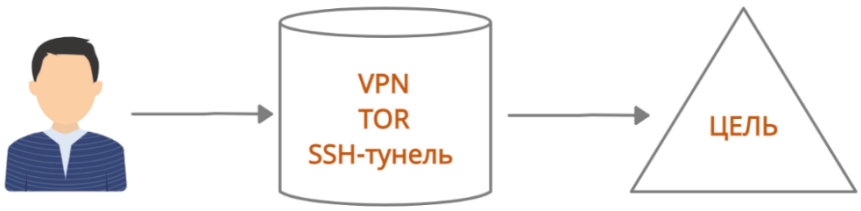


Рисунок 1. Схема базового уровня защиты

Данная схема – это всего лишь продвинутая альтернатива прокси, основная задача которой подменить Ваш настоящий IP-адрес. Такая схема поможет Вам всего лишь попасть на ресурс, предназначенный для другой страны, поэтому рассчитывать на безопасность при таком уровне защиты уж точно не приходится. Ведь всего один неверный шаг и Ваш реальный IP-адрес станет известен системе со всеми вытекающими последствиями. Основными типами уязвимости для такой схемы являются:

1. Компрометация узла, или простыми словами, получение доступа к закрытой информации постороннего лица

2. Отпечатки пальцев, так называемые fingerprints, то есть следы, оставляемые в сети пользователем, например, версия его браузера или часовой пояс
3. Анализ логов у провайдера и в дата-центре

Очень часто в сети Вы можете заметить статьи о частном VPN, что такая технология позволит создать качественный отпечаток Вашей личности в интернете. Спешу Вас заверить, что данная информация является очередной уловкой для обывателя данной области. Рассмотрим на примере, кому-то известен Ваш внешний IP, дата-центр, а уже дата-центру известно, какому серверу этот IP принадлежит. Сложно ли установить с какого реального IP к этому серверу подключались? Если Вы один клиент? Ответ очевиден. Когда клиентов, например 100, 1000 - тут уже все намного сложнее.

Рассматривая такую технологию, как TOR, необходимо упомянуть, что, во-первых, используя данную технологию Вы уже вызываете подозрение у провайдера, а во-вторых, более 1000 выходных нод известны и заблокированы. Многие сайты, видя, что Вы используете TOR, расценивают это как попытку нарушения безопасности и за Вами ведётся более пристальное внимание. Это как, когда Вы в подростковом возрасте забегаете в магазин техники. Сотрудники магазина то и дело смотрят за каждым Вашим шагом, ведь они отвечают за товар в данном магазине. Тем более, на многих сайтах попросту стоят файерволы, чтобы не допустить пользователя к содержимому сайта. Кроме всего вышеперечисленного, скорость работы TOR намного ниже VPN, а нам, привыкшим к хорошим скоростям пользователям, будет весьма сложно работать при таких условиях.

Итог: Если Вы просто хотите обходить простейшие запреты на сайты, при этом, не жертвуя скоростью работы, имея отличное соединение и возможность пускать трафик через другой узел, то Вам необходимо воспользоваться VPN. Причём, здесь Вы можете воспользоваться как платным сервисом, так и бесплатными аналогами.

Для Вас, скорее всего, использование технологии TOR будет излишним, но и он способен решить некоторые задачи, особенно имея дополнительный слой безопасности, такой как VPN или SSH-туннель.

Средний уровень защиты

Такой уровень является оптимальным для работы. Про него можно сказать, что сочетание технологий дополнило и улучшило каждую из них. Конечно, узнать Ваш реальный адрес будет затруднительно, но атаки, которым был подвержен предыдущий уровень защиты, здесь также остаются, ведь Ваш компьютер всё ещё остается уязвимым местом.

Схема среднего уровня защиты показана на рисунке 2.

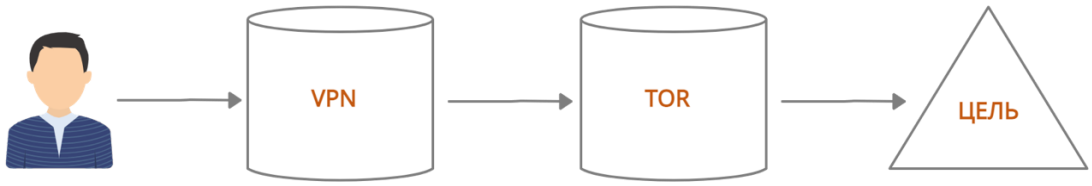


Рисунок 2. Схема среднего уровня защиты

Высокий уровень защиты

При использовании высокого уровня защиты рабочий компьютер должен быть уже не Ваш, а удалённый, с другой операционной системой, другим браузером, плагинами, парой кодеков, но важнейшей частью является то, что никакой уникальности, в виде необычных шрифтов и так далее, не должно быть в данном случае. Даже если произойдёт утечка или компрометация системы, то клиент всё равно остаётся прикрыт ещё одним VPN.

Схема высокого уровня защиты показана на рисунке 3.

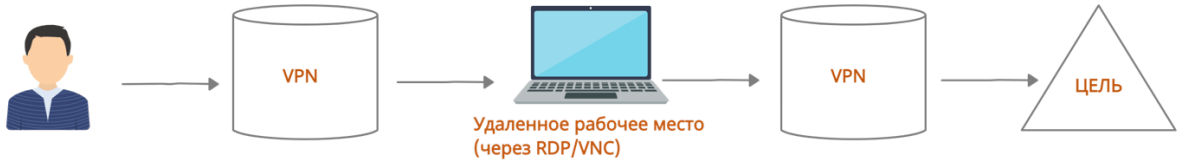


Рисунок 3. Схема высокого уровня защиты

Максимальный уровень защиты

Такой подход предполагает первичное подключение к VPN и вторичное подключение к VPN. Это позволит в случае, если первый VPN будет скомпрометирован, в связи с какой-либо утечкой, скрыть трафик от провайдера с целью не выдать реальный IP-адрес в дата-центре с удалённым рабочим местом. Затем в рассматриваемой схеме вступает в силу установленная виртуальная машина на удалённом рабочем месте. Это позволяет каждую загрузку делать откат к стандартной системе с банальным набором дополнений и плагинов.

Безусловно, о высокой скорости работы тут и речи идти не может, но тот уровень безопасности, который тебе предоставляет данный уровень защиты, стоит того.

Схема максимального уровня защиты показана на рисунке 4.

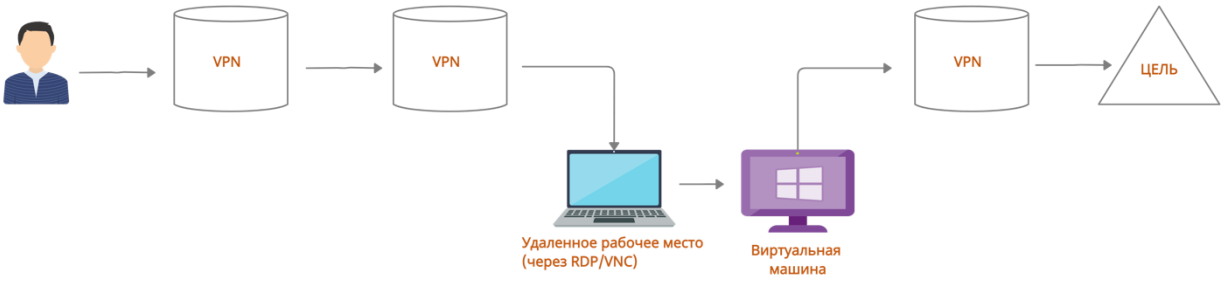


Рисунок 4. Схема максимального уровня защиты

Для повышения неуязвимости при использовании данного уровня защиты необходимо также добавить добавить автоматическое посещение веб-сайтов в фоновом режиме, с Вашей реальной машины как имитацию серфинга, чтобы не было подозрения, что используется какое-то средство анонимизации.

Залог успеха в сохранении анонимности – это разделение работы с секретными и персональными данными. Все вышеописанные схемы будут бесполезны, если, например, зайти в свой почтовый ящик или открыть аккаунт в социальной сети.

Подмена MAC-адреса сетевого адаптера

Доступный интернет стал в первую очередь огромным средством экономии денег, так как у каждого из нас появилась возможность выхода в сеть, не расходуя свой трафик и, соответственно, деньги. Интернет стал доступен в метро, автобусах, кафе, даже у ларьков с быстрым питанием есть своя точка доступа.

Соответственно, и количество мошенничества выросло, благодаря такой доступности интернета. Именно поэтому, опытные пользователи стали подменять свой MAC-адрес.

Абсолютно у любого устройства, выходящего в сеть, имеется свой MAC-адрес, причём он является уникальным и позволяет однозначно идентифицировать устройство в сети. Такой адрес иногда называется физическим или аппаратным адресом, который

устанавливается на заводе изготовителя, но, как правило, имеется возможность изменить его программными средствами.

Если говорить простыми словами, то на низшем уровне сети, сетевые интерфейсы, подключённые к сети, связываются друг с другом при помощи MAC-адресов. То есть, когда Вы хотите открыть страницу какого-либо сайта, то данный запрос обрабатывается несколькими уровнями модели TCP/IP. Введённый адрес в адресной строке преобразуется из буквенного вида в цифровой IP-адрес, который с помощью запроса передается сначала на маршрутизатор, а потом интернет. Но если рассматривать данную процедуру на низшем уровне, то сетевая карта ищет другие MAC-адреса для интерфейсов в той же сети. По факту она знает только как отправить запрос на сетевой интерфейс маршрутизатора.

Другие цели использования MAC-адреса:

1. Отслеживание устройств: так как он уникален, его можно использовать для отслеживания. Например, Вы забыли отключить функцию автоматического подключения к открытым сетям, Ваш телефон будет сам подключаться и передавать MAC-адрес. Затем, методом простого анализа данных, можно определить, где Вы были в течение дня.
2. Идентификация устройств: многие общественные сети используют его для идентификации устройства, чтобы заблокировать Вам доступ через определённый промежуток времени. Для снятия этого ограничения достаточно лишь сменить MAC-адрес.
3. MAC-аутентификация: некоторые провайдеры могут активировать проверку подлинности и разрешать подключаться к сети только устройствам с определённым MAC-адресом.
4. Фильтрация MAC-адресов.
5. Статический IP-адрес: при подключении устройства с указанным у провайдера MAC-адресом, оно всегда будет получать один и тот же IP-адрес.

Также, необходимо заметить, что у каждого сетевого интерфейса свой MAC-адрес. Поэтому у ноутбука, который имеет как беспроводной вариант подключения к сети, так и проводной, есть, как минимум, 2 уникальных MAC-адреса.

ИСПОЛЬЗОВАНИЕ ROOTKIT

Соловьев Грант Саргисович, курсант 4 курса
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Rootkit — набор программных средств (например, исполняемых файлов, скриптов, конфигурационных файлов), для обеспечения маскировки объектов (процессов, файлов, директорий, драйверов), управления (событий, происходящих в системе), сбора данных (параметров системы).

Часто программы, обеспечивающие удаленный доступ к компьютеру-жертве или прослушивание пакетов в сети, также входят в состав rootkit. Обязательно в составе rootkit будут средства, «прикрывающие» его: файлы и каталоги, которые вы укажете. Функции rootkit ограничиваются только его создателем

Rootkit можно классифицировать по механизму, который используется для заражения компьютера. Цель заражения определяется уровнем привилегий, который получает атакующий.

Существуют так называемые кольца защиты процессора:

- кольцо 3 – режим пользователя (прикладные программы);

-кольцо 2 – режим системного управления (драйверы);

-кольцо 1 – режим гипервизора (обеспечивает возможность запуска нескольких операционных систем, изолированных друг от друга, на одной машине);

-кольцо 0 – режим супервизора (выполнение ядра операционной системы).

Все программы взаимодействуют с системой через вызовы. В зависимости от программы она может посылать вызовы к нулевому кольцу или к 3 кольцу (уровень приложений).

Программы, которые работают на уровне пользователя используют API (Application Programming Interface) для запросов к ресурсам операционной системы. Эти запросы поступают к ядру через DLL (Dynamic Link Libraries), они преобразуют API вызовы в код, понятный для ядра. То есть, на пользовательском уровне используется посредник для «общения» с ядром операционной системы. К базовым нуждам любой программы можно отнести чтение и запись данных на носителе. Для более эффективной работы каждая пользовательская программа создает свою таблицу, которая содержит адреса всех API или системных функций, которые ей необходимы для выполнения. Эта таблица называется IAT (Import Address Table). IAT является неотъемлемой частью программы, которая загружается в память.

Косвенные вызовы, которые использует программа пользовательского уровня, ограничивают Rootkit пользовательского уровня, которые могут работать только в рамках другого приложения или как отдельная программа пользовательского уровня. Rootkit пользовательского уровня хранятся в адресном пространстве пользовательских программ и могут быть обнаружены обычными программами безопасности, которые работают в режиме ядра.

Для того, чтобы получить доступ к машине на Linux необходимо модифицировать сервисы «login», «sshd», «inetd» и т.д. Злоумышленник просто должен получить доступ к этим сервисам и предоставить бэкдор пароль, чтобы получить root доступ. Различные сервисы, отображающие информацию о процессе, запущенном на машине, такие как «ps», «pidof», «top» изменяются таким образом, чтобы вредоносный процесс не был указан среди других запущенных процессов. Кроме того, команда «killall» обычно изменяется так, чтобы вредоносный процесс не мог быть завершен, а команда «crontab» изменяется так, чтобы вредоносный процесс запускался в определенное время без каких-либо изменений

конфигурации «cron». «Netstat» также изменяется таким образом, чтобы не показывать никакой информации о портах, которые использует злоумышленник. Также злоумышленник изменяет «ls» и «find», чтобы его файлы не были обнаружены пользователем. Модифицируется «du», чтобы скрыть файл из коллекции использования диска. Модифицируется «syslog» для того, чтобы не регистрировались события на целевой машине.

Несмотря на недостатки Rootkit пользовательского уровня намного легче программировать, чем Rootkit уровня ядра и поэтому они с меньшей вероятностью смогут нанести вред операционной системе и пользователю.

Ядро операционной системы является «мозгом» операционной системы, базовым ее компонентом. Ядро обеспечивает контроль и функционал для всех программ, которые запускаются на машине. Оно поддерживает и управляет многими системными ресурсами и функциями, такими как память, безопасность и планирование процессов – облегчает связь между программным обеспечением и аппаратными средствами.

В отличие от Rootkit пользовательского уровня, которые работают на 3 кольце, Rootkit уровня ядра работает на 0 кольце и взаимодействуют путем перехвата собственных (уровня ядра) API. Ядро имеет глобальный доступ к каждому уголку операционной системы поэтому это лучшее место для использования Rootkit. Оттуда Rootkit может получить доступ к любой ячейке памяти и любому аппаратному обеспечению, изменить код ядра, модифицировать критическую структуру данных, которую ядро использует для отслеживания активности. Таким образом, Rootkit уровня ядра оказывает влияние на всю систему, что делает их намного более опасными, чем Rootkit пользовательского уровня.

После установки Rootkit уровня ядра перенаправляет вызовы системных функций, таким образом, что вместо кода ядра, выполняется его собственный код. Один из методов, который использует Rootkit, чтобы изменить обычный путь выполнения программы известен как hooking – это перехват вызовов системных функций и корректировка результатов, для сокрытия активности. Hooking позволяет перенаправить нормальный поток выполнения программы на функции, которые содержит Rootkit.

Как в пользовательском режиме, так и в режиме ядра Rootkit используют hooking для фильтрации результатов, которые возвращаются операционной системой и создают иллюзию незараженной системы. Rootkit прячут используемые ими порты, процессы, файлы реестра, которые нельзя обнаружить большинством программ, предназначенных для обнаружения Rootkit. Так происходит потому, что данные программы полагаются на данные, предоставленные операционной системой. Например, если пользователь пытается обнаружить Rootkit в диспетчере задач, проводнике, реестре, проверить открытые порты то он ничего там не увидит.

Операционная система Windows использует множество таблиц данных для хранения и слежения за важной системной информацией. Эти таблицы могут быть перенесены или изменены с помощью Rootkit. Rootkit уровня ядра и пользовательского уровня используют hooking, однако, их функционал ограничен их привилегиями.

Некоторые Rootkit обладают собственным «антивирусом». Они могут обнаруживать программу-сканер и переставать работать или блокировать запуск данной программы.

Однако, очень сложно реализовать Rootkit уровня ядра без нарушения баланса системного ядра. Rootkit уровня ядра часто обнаруживается пользователем из-за нарушения стабильности работы операционной системы и ошибок (в случае, если Rootkit был небрежно написан).

Еще одной особенностью Rootkit является их устойчивость к перезапуску системы. Для того, чтобы пережить перезагрузку Rootkit должен загрузиться на накопитель и добавить запись автозапуска в реестр, таким образом, при запуске машины Rootkit автоматически загружается в память. В данном случае появляется возможность обнаружения Rootkit, конечно, если он не умеет скрывать себя. Rootkit, которые не

обладают устойчивостью к перезапуску, существуют только в оперативной памяти и полностью исчезают после перезапуска машины. Однако данный Rootkit будет продуктивен только на машине, которую редко перезагружают, например сервер, подключенный к большому количеству клиентских машин.

Список использованных источников

1. Батаев, А.В. Операционные системы и среды: Учебник / А.В. Батаев, Н.Ю. Налютин, С.В. Синицын и др. - М.: Academia, 2018. - 271 с.
2. Дроздов, С.Н. Операционные системы: Учебное пособие / С.Н. Дроздов. - Рн/Д: Феникс, 2018. - 480 с.
3. Пилон, Д. Управление разработкой ПО / Д. Пилон. - М.: Питер, 2014. - 402 с.

БРАНДМАУЭР

Стародубцев Валентин Юрьевич курсант 1 курса
Научный руководитель Овчинский Анатолий Семёнович профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Мой брандмауэр защищает меня от заражения при "попутной загрузке"

Этот тезис ложен. Брандмауэры – это важная составляющая защиты компьютера. Однако невозможно защитить ПК от заражений при "попутной загрузке" с помощью одного лишь брандмауэра. Для полной и эффективной защиты интернет-пользователь должен дополнительно установить комплексное решение безопасности с интегрированной Web-защитой. При успешном заражении компьютера брандмауэр не всегда может предотвратить выполнение вредоносных задании вредоносной программой.

Брандма́уэр. О брандмауэре многие узнают при попытке установить приложение или при появлении окошка, оповещающего об опасности. И тут начинают возникать вопросы: что это, для чего нужно, как выключить/включить, настроить. Мы расскажем все про брандмауэр — что это такое в компьютере, где найти, как и зачем использовать. Даже новички научатся решать проблемы и эффективно защитят операционку от вирусов.

Что такое брандмауэр и какие функции выполняет

С немецкого брандмауэр (brandmauer) переводится как “противопожарная стена”. Определение перекочевало из сферы строительства в информатику, где означает программу, главная функция которой — защита операционной системы от сетевых, хакерских атак. Назначение брандмауэра — выслеживать и блокировать все вредоносные подключения, обеспечивать защиту персональной пользовательской информации. То есть он постоянно прослушивает порты компьютера, чтобы выявить момент подключения к ним нехороших прог, вирусов, червей.

Каковы функции такой защиты:

- следит за сомнительными соединениями, например, если они пытаются отправить информацию в Интернет;
- блокирует порты, которые не участвуют в работе, и изучает трафик с открытых портов;
- наблюдает за работающими приложениями и предупреждает пользователя, если изменяется важная информация запущенных прежде программ.

Вывод: Файрвол — нужная прога для защиты компьютерной системы от вредоносных атак. Правильная настройка помогает избежать трудностей при использовании Интернета и приложений. Следует убедиться в том, что компьютер и пользовательские данные надежно защищены.

Для продвинутых пользователей есть брандмауэры сторонних производителей, которые отличаются высокой мощностью и расширенными настройками. Лучше поставить комплексную защиту — файрвол вместе с антивирусом. Такие программы как Kaspersky Internet Security и Avast! Internet Security обеспечивают полную безопасность. Даже самые сильные сетевые атаки не смогут нанести ущерб!

ИДЕНТИФИКАЦИЯ

Терехов Александр Сергеевич, студент 2-го курса

Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук

Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Криминалистика появилась как наука, по определению истины в уголовном судопроизводстве. Она изучает законность объективной действительности, которая проявляется в работе по раскрытию и расследованию преступлений.

Одним из главных методов установления истины в уголовном судопроизводстве, когда возникает необходимость определить связь подозреваемого, принадлежащих ему предметов и других объектов с расследуемым событием по оставленным следам и иным материальным отображениям, является криминалистическая идентификация.

Во время совершения преступления преступник взаимодействует определенным способом с окружающей средой оставляя следы, в которых отражаются внешние признаки человека: следы рук, ног; последствия использования орудий преступления.

Значение идентификации заключается в том, чтобы по следам установить объект. Объектом может служить человек, часть одежды, обувь, орудия совершения преступления, транспорт и др. В качестве следов могут быть документы, мысленные образы и др.

Криминалистическая идентификация основывается на нахождение и признание оригинальных признаков объектов. Признаки, показывающие свойства объекта, которые необходимы для его отождествления, называют идентификационными.

Чтобы быть идентификационным, признак объекта должен:

1) Быть особенным, оригинальным (точное отражение свойств определённого объекта).

2) Быть достаточно устойчивыми (не изменяться в течение времени)

3)Частота встречаемости признака (чем реже встречается признак, тем легче идентифицировать объект)

Идентификационные признаки подразделяются:

1) на общие и частные;
2) на качественные и количественные.

Общие отражают наиболее существенные, постоянные свойства объектов (их групп): форму, размеры, цвет, назначение. Частные — это специфические свойства объекта, выделяющие его из других объектов. Качественные (атрибутивные) определяются качественными характеристиками (например, петлевой папиллярный узор) и количественные определяются числом (например, размер следа, количество патронов)

Технологии 21 века способствуют распознаванию личности по найденным на месте преступления образцам ДНК. Но требуется значительное время для распознавания. Достаточно сравнить ДНК, подозреваемых с ДНК, найденной на месте преступления и доказано принадлежащей преступнику. Идентификация личности на основании данных ДНК-анализа в криминалистике выполняет две задачи:

1) анализ био. образцов, найденные на месте преступления, с образцами, полученными от подозреваемого.
2) установление сходства по признакам ДНК.

В качестве материала ДНК могут быть найдены на месте преступления кровь, моча, волосы.

Также, используется биометрия лица для поисков преступников. С камер на подъездах, в общественных транспортах, на светофорах, в переулках, в аэропортах сравнивается с базами данных, в которых храниться лица преступников.

Во время изоляции в России использовали систему распознавания лиц «Визирь» для поиска нарушителей карантина. Лица, поставленные на самоизоляцию, были занесены в определенный реестр данных, но штраф выписывался не автоматически, а сотрудниками.

Результат биометрических технологий, оценивается на использовании двух вероятностей - ошибка ложного отказа и ошибка ложного подтверждения. Ошибка ложного отказа возникает в случае, если система не опознала биометрический признак, который соответствует имеющемуся в ней шаблону. Например, Иванова А.А. не распознан, как Иванов А.А., а ошибка ложного подтверждения - случае, если система неверно подтвердила предъявленный ей признак с не соответствующим ему на самом деле шаблоном, например, система показала Петрова В.В. вместо Иванова А.А.

Вывод: Процесс никогда не будет стоять на месте и будет лишь прогрессировать, давая новые методы и усовершенствования старые идентификации личности. Мы находимся на переходном этапе информатизации множество процессов. Лет через 10-20 мы будем жить в умных городах, осуществляя на биометрическом уровне поиска, с помощью камер, установленных в аэропортах, метро, улицах, общественном транспорте; на местах преступлениях будет осуществлена на местах проверка ДНК, без участия лабораторий.

Список использованных источников

1. Ищенко Е.П., Топорков А.А. Криминалистика: Учебник. — 2-е издание. — М.: Юридическая фирма "КОНТРАКТ", ИНФРА-М, 2010.
2. Колдин В.Я. Судебная идентификация. М., ЛексЭст, 2002.
3. Селиванов Н.А., Эйсман А.А., Грабовский В.Д. и др. Идентификация и дифференциация в структуре деятельности по выявлению, раскрытию и расследованию преступлений: Учебное пособие. Горький, 1980.

ПРОГНОЗИРОВАНИЕ ЗАДАЧ МАРКЕТОЛОГА В СТРАХОВОЙ КОМПАНИИ С ВИЗУАЛИЗАЦИЕЙ ОСНОВНЫХ ПРОЦЕССОВ

Торшин Андрей Игоревич, студент 3 курса
Научный руководитель Назарова Ольга Игоревна, преподаватель
Старооскольский технологический институт им. А.А. Угарова(филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В настоящее время для обеспечение должной безопасности и эффективности работы с клиентскими данными необходимо создавать информационные системы. Потребность создания информационной системы является прогнозирование задач маркетолога в страховой компании.

Актуальность данной темы заключается в совершенствовании маркетинга и менеджмента страховой компании в настоящих рыночных реалиях.

Прогнозирование – научно обоснованное предсказание вероятностного развития событий или явлений на будущее на основе статистических, социальных, экономических и других исследований.

На основе проведенного анализа предметной области была построена диаграмма входных/выходных данных, представленная на рисунке 1.

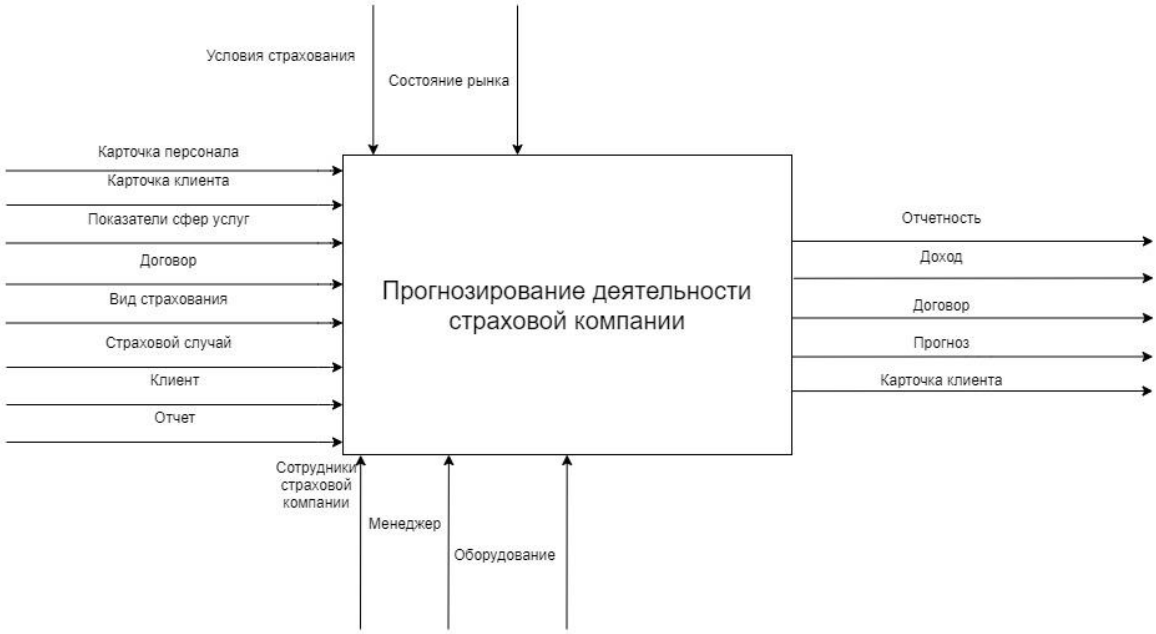


Рисунок 1 – Диаграмма входных/выходных данных

На диаграмме входных/выходных данных изображены входные данные: карточка клиента, карточка персонала, показатели сфер услуг, договор, вид страхования, страховой случай, клиент, отчет; выходные данные: отчетность, доход, прогноз, дополненная карточка клиента. На основе входных и выходных данных была реализована диаграмма декомпозиции рассматриваемой области, представлена на рисунке 6.

Входные данные – это числовые, текстовые, графические и другие данные, получаемые информационной системой из различных внешних источников [4].

Выходные данные – это отображение того, что получается в результате манипуляций программы [4].

Для разработки программного приложения было выбрано приложение MS Visual Studio 2017 на языке C# и СУБД SQL Server Management Studio. Данное решение было выбрано из–за таких достоинств как:

– информативный вывод ошибок и возможность программы самой решить их;
– широкий спектр возможностей с помощью предустановленных объектах и их свойствах;
– визуализация внешнего вида программы;
– использование точек остановы;
– возможность кастомизации программного приложения.

При инициализации приложения перед пользователем представиться форма авторизации, изображенной на рисунке 2.

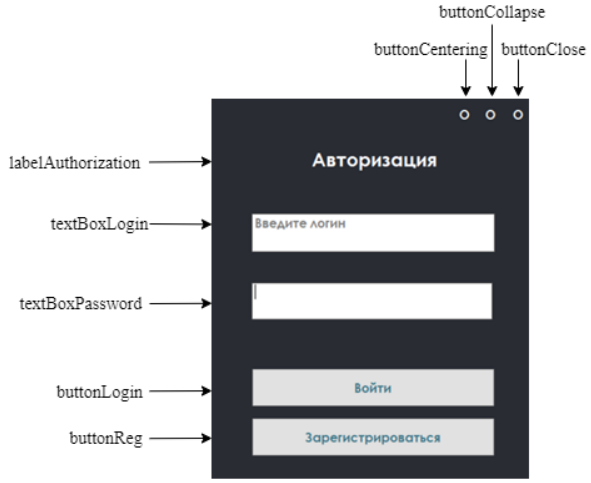


Рисунок 2 – Форма авторизации

Главная форма представлена на рисунке 3.

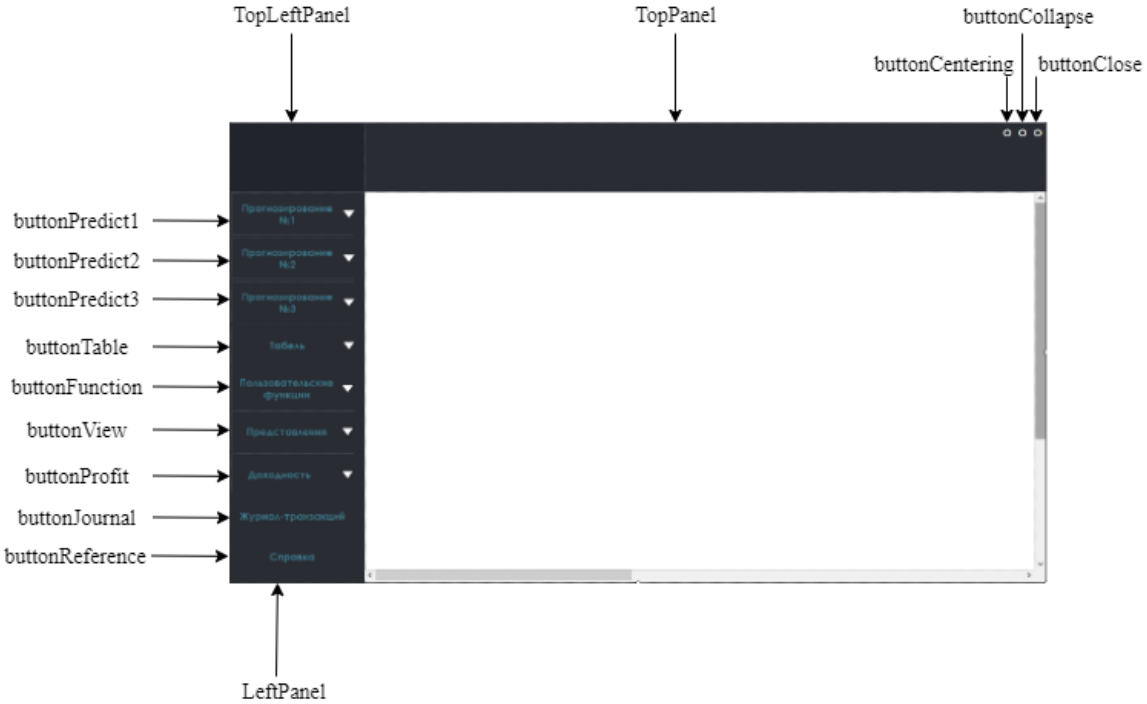


Рисунок 3 – Главная Форма

Пример работы «Прогнозирования №1» изображен на рисунке 4.

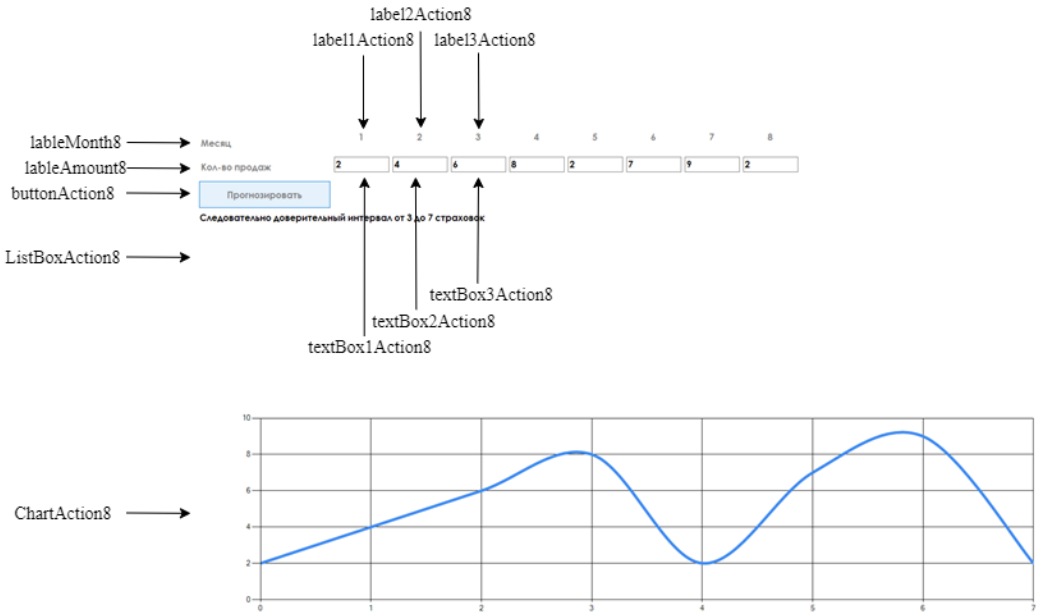


Рисунок 4 – Пример работы «Прогнозирования №1»

Пример работы «Прогнозирования №2» изображен на рисунке 5.

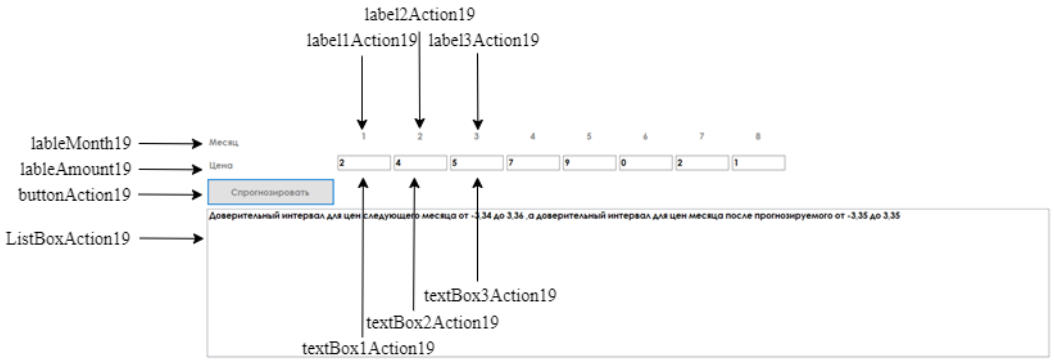


Рисунок 5 – Пример работы «Прогнозирование №2»

Пример работы «Прогнозирования №3» изображен на рисунке 6.

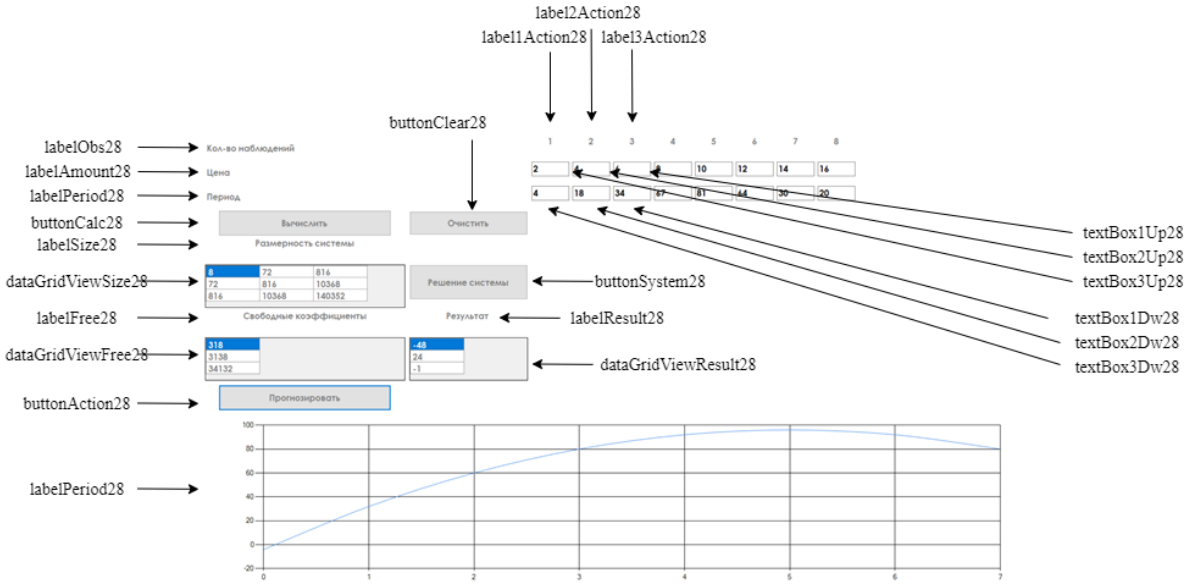


Рисунок 6 – Пример работы «Прогнозирование №3»

В результате выполнения исследовательской работы была разработана информационная система для прогнозирования задач маркетолога в страховой компании с визуализацией основных процессов.
Были решены следующие задачи:
– реализовано прогнозирование задач маркетолога страховой компании;
– реализована возможность внесения, хранения, учета данных в базе данных страховой компании;
– реализована возможность автоматического решения математических моделей с визуализацией основных процессов.
– осуществлено занесение информации в базу данных;
– реализовано выполнение модификации и удаления информации из базы данных;
– создана поддержка целостности базы данных, не допуская появления некорректных данных;
– создан контроль вводимых данных;
– реализована возможность накопления и хранения статистики о деятельности предприятия;
– создана возможность решения математических моделей;
– реализована визуализация математических моделей.

Список использованных источников

1. Гагарина, Л. Г. Технология разработки программного обеспечения: учебное пособие / Л.Г. Гагарина, Е.В. Кокорева, Б.Д. Сидорова-Виснадул ; под ред. Л.Г. Гагариной. — Москва: ФОРУМ: ИНФРА-М, 2020. — 400 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0812-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/1067012
2. Гвоздева, В. А. Основы построения автоматизированных информационных систем : учебник / В.А. Гвоздева, И.Ю. Лаврентьева. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2018. —318 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0705-4. - Текст : электронный. - URL: https://znanium.com/catalog/product/922734
3. Чистов Д.В. Проектирование информационных систем : учебник и практикум для среднего профессионального образования / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук ; под общей редакцией Д. В. Чистова. — Москва : Издательство Юрайт, 2018. — 258 с. — (Профессиональное образование). — ISBN 978-5-534-03173-7. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414925
4. КиберФорум – форум программистов, системных администраторов, администраторов баз данных, компьютерный форум, форум по электронике и бытовой технике, обсуждение софта. [Электронный ресурс], [сайт]. — URL: https://www.cyberforum.ru/

КИБЕР-ТЕХНОЛОГИИ, КАК ОДНО ИЗ СРЕДСТВ СОВЕРЕШЕНИЯ ПРЕСТУПЛЕНИЙ

Трипунов Артем Вячеславович, курсант 4-го курса
Научный руководитель Казанцев Владимир Иванович преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Информационные технологии содержат много средств: для обмана, краж и других противоправных действий.

Кибер-преступность – это незаконная деятельность, совершаемая с помощью электронных устройств (компьютеров, планшетов, смартфонов) через коммуникационные сети в информационном пространстве. Под информационным пространством подразумеваются информационно-телекоммуникационные сети (например, Интернет), компьютерные локальные сети и т. д.

Развитие технологий в современном мире обуславливает их проникновение во все сферы общественной жизни. Этим пользуются не только добросовестные пользователи коммуникационных сетей, но и злоумышленники, преследующие различные противоправные цели, одной из главных целей является получение материальных средств, то бишь денег. Регистрируются преступления, связанные с хищением денежных средств из банков и иных кредитных организаций, у физических и юридических лиц, совершаемых с использованием современных информационно-коммуникационных технологий.

Мошенники используют различные способы обмана людей в интернете: от спама, фишинга до создания сайтов-двойников. Цель злоумышленников — украсть что-то ценное и использовать себе во благо либо скомпрометировать или обрушить чужой бизнес, для этого крадутся номера банковских карт, данные паспорта, номера телефонов.

Фишинг-мошенничество – это попытки мошенников (хакеров, злоумышленников) обмануть человека, с целью выведать любую конфиденциальную информацию, начиная от имени пользователя и заканчивая банковскими данными. Как описано выше, фишинг-мошенники сосредоточены на достижении цели получить вашу информацию удаленно. Они пытаются заставить людей самостоятельно ввести регистрационные данные и передать их на сервер мошеннику.

Таким образом, можно выделить высокую общественную опасность киберпреступлений уже в период их становления и развития. Хотя тогда не существовало интеллектуальных систем защиты информации, а сами преступления выражались в большинстве своем во внешнем контакте с хранилищами информации (в целях уничтожения, неправомерного доступа, копирования, изменения информации). В данное время отмечаются высокие актуальность и общественная опасность киберпреступлений. Сейчас преступление является сильно латентным, может выражаться в совершении «традиционных» противоправных деяний (но в сфере киберпространства либо с использованием кибер-технологий) и значительной сложностью расследования (в частности, мы имеем в виду трудность поиска преступников и возмещения ущерба). Кроме этого, появился и третий фактор - масштабность, т. е. киберпреступления совершаются везде, где есть Интернет, сетевые структуры или информационные технологии, поэтому так важно обеспечить

эффективную и оптимальную уголовно-правовую политику в борьбе с данным видом преступности на международном уровне.

МЕТОДИКА ЗАЩИТЫ ОПЕРАЦИОННОЙ СИСТЕМЫ WINDOWS ОТ ВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Трубицин Михаил Олегович, командир отделения 4-го курса
Научный руководитель, Казанцев Владимир Иванович преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г.Москва

Компьютерные вирусы создают множество проблем для многих пользователей. И все они в подавляющем большинстве случаев устанавливали антивирус. Вывод один - антивирус не обеспечивает необходимого уровня защиты. Эта проблема требует сложной настройки компьютера и изучения основ безопасности.

Вирус — это вредоносная программа, созданная злоумышленником. Целью первых вирусов было самоутверждение своих создателей, а их действия заключались в нанесении вреда компьютеру. Сегодня подавляющее большинство вирусов нацелены на получение тем или иным способом незаконных денег.

Чтобы эффективно защитить себя от вирусов, нужно придерживаться определенных правил:

Используйте антивирусное ПО: установите антивирусное ПО и регулярно обновляйте его. Это поможет защитить ваш компьютер от вирусов и других вредоносных программ. Программы защиты от вредоносных программ ищут вирусы, шпионское ПО и другие вредоносные программы, которые пытаются получить доступ к вашей электронной почте, операционной системе или файлу. Регулярно проверяйте и обновляйте веб-сайт поставщика вредоносных программ, так как новые угрозы могут возникать каждый день.

Не открывайте электронные письма от неизвестных отправителей или неизвестные вложения. Многие вирусы передаются в виде вложений электронной почты, которые открывают вложения для распространения. Мы настоятельно рекомендуем открывать только ожидающие или известные вложения.

Используйте в своем браузере блокировщик всплывающих окон. Всплывающие окна — это небольшие окна в браузере, которые появляются в верхней части просматриваемой веб-страницы. Большинство этих окон используются в рекламных целях, но могут содержать вредоносный код. Блокировщик всплывающих окон позволяет избавиться от некоторых или даже всех окон.

Обратите внимание на уведомление Windows SmartScreen. Будьте осторожны с неизвестными программами, загруженными из Интернета. Эти приложения могут быть скомпрометированы. Когда вы загружаете и запускаете приложение из Интернета, SmartScreen использует информацию о вашей репутации, чтобы предупредить вас о том, что приложение может быть нераспознаваемым или вредоносным.

Держите Windows в актуальном состоянии. Microsoft периодически выпускает некоторые обновления безопасности, чтобы обеспечить вашу безопасность. Обновления могут предотвращать вирусы и другие вредоносные атаки, блокируя уязвимости системы безопасности.

Используйте брандмауэр. Брандмауэр Windows или другое программное обеспечение брандмауэра уведомит вас о подозрительной активности, когда вирус или червь попытается подключиться к вашему компьютеру. Это позволяет блокировать вирусы, черви и злоумышленников, которые доставляют программы, которые могут угрожать вашему компьютеру.

Используйте настройки конфиденциальности вашего браузера. Некоторые веб-сайты могут пытаться использовать вашу личную информацию для целевой рекламы, мошенничества или кражи личных данных.

Убедитесь, что управление учетной записью пользователя включено. Если вы внесете в свой компьютер изменения, требующие прав администратора, система управления учетными записями пользователей уведомит вас и попросит подтвердить изменения. Контроль учетных записей пользователей предотвращает внесение вирусом нежелательных изменений. Чтобы открыть элемент управления учетной записью пользователя, проведите пальцем от правого края экрана и нажмите «Поиск». В поле поиска введите Контроль учетных записей пользователей и выберите «Изменить настройки контроля учетных записей пользователей».

Очистите интернет-кеш и историю браузера. Большинство браузеров хранят информацию о посещаемых вами веб-сайтах (ваше имя, адрес и т. д.). Может быть полезно сохранить эту информацию на вашем компьютере, но, например, если вы используете общедоступный компьютер и не хотите оставлять на нем свою личную информацию, вам может потребоваться удалить ее часть или все.

Убедитесь, что SmartScreen включен при использовании Microsoft Edge. SmartScreen в Microsoft Edge предупреждает вас о потенциально опасных веб-сайтах или местах загрузки и помогает защитить вас от фишинга и атак вредоносного ПО.

Большой не всегда лучше. Одновременный запуск нескольких программ против вредоносных программ может вызвать замедление работы системы или ее нестабильность. Установка анти-стороннего программного обеспечения автоматически отключит Microsoft Defender. Если установлены две сторонние программы защиты от несанкционированного доступа, они могут работать одновременно.

Если следовать всем этим простым правилам, то ваш персональный компьютер будет в безопасности, работать исправно и ваша информация будет под защитой.

Список использованных источников

1. Мартемьянов, Ю.Ф. Операционные системы. Концепции построения и обеспечение безопасностиюУчебное пособие / Ю.Ф. Мартемьянов. - М.: Горячая линия -Телеком, 2017. - 332 с.
2. Матросов, В.Л. Операционные системы, сети и интернет-технологии: Учебник / В.Л. Матросов. - М.: Academia, 2017. - 1040 с.

ОБРАБОТКА ИЗОБРАЖЕНИЙ И КОМПЬЮТЕРНОЕ ЗРЕНИЕ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЯХ

Уйнук-оол Роза Омаковна, курсант 4-го курса
Научный руководитель, Казанцев Владимир Иванович, Преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Компьютерное зрение было расширено на обширную область поля, начиная от записи необработанных данных и заканчивая извлечением паттерна изображения и интерпретацией информации. Она представляет собой комбинацию концепций, методов и идей цифровой обработки изображений, распознавания образов, искусственного интеллекта и компьютерной графики. Большинство задач в области компьютерного зрения связаны с процессом получения информации о событиях или описаниях из входных сцен (цифровых изображений) и извлечения признаков. Методы, используемые для решения задач компьютерного зрения, зависят от области применения и характера анализируемых данных.

Компьютерное зрение-это сочетание обработки изображений и распознавания образов. Результатом процесса компьютерного зрения является понимание образа. Развитие этой области осуществляется путем адаптации способности человеческого зрения к восприятию информации. Компьютерное зрение-это дисциплина извлечения информации из изображений, в отличие от компьютерной графики . Развитие компьютерного зрения зависит от системы компьютерных технологий, будь то улучшение качества изображения или распознавание изображений. Существует перекрытие с обработкой изображений по основным методикам, и некоторые авторы используют оба термина взаимозаменяемо.

Основной целью компьютерного зрения является создание моделей и извлечение данных и информации из изображений, в то время как Обработка изображений заключается в реализации вычислительных преобразований изображений, таких как резкость, контрастность и другие. Он также имеет сходное значение и иногда перекрывается, фокусируется на полном дизайне, интерфейсе и всех аспектах технологий, связанных с взаимодействием человека и компьютера. Затем развивается как отдельная дисциплина (которая является областью междисциплинарной науки), в которой обсуждаются взаимосвязи между человеком и компьютером, опосредованные развитием технологий, включая человеческие аспекты. Функционально компьютерное зрение и человеческое зрение-это одно и то же, причем цель интерпретации пространственных данных, то есть данных, индексированных более чем одним измерением. Однако нельзя ожидать, что компьютерное зрение будет воспроизводиться точно так же, как человеческий глаз.

Это связано с тем, что система компьютерного зрения имеет ограниченные характеристики и функции по сравнению с человеческим глазом. Несмотря на то, что многие ученые предложили широкую область методов компьютерного зрения для воспроизведения человеческого глаза, тем не менее, во многих случаях существуют какие-либо ограничения производительности системы компьютерного зрения. Одной из существенных проблем в их методике является чувствительность параметров, прочность алгоритма и точность результатов. Это влияет на сложность оценки производительности систем компьютерного зрения. Как правило, оценка производительности включает в себя измерение некоторых основных характеристик алгоритма для достижения точности, прочности или расширяемости для контроля и мониторинга производительности системы.

Поскольку производительность системы компьютерного зрения зависит от конструкции прикладной системы, многие ученые предлагают комплексные усилия по расширению и классификации компьютерного зрения во многих областях и конкретных приложениях, таких как автоматизация на сборочной линии, дистанционное зондирование,

робототехника, компьютерные и человеческие коммуникации, инструменты для слабовидящих и другие.

Компьютерное зрение работает с помощью алгоритма и оптических датчиков, стимулирующих визуализацию человека для автоматического извлечения ценной информации из объекта. По сравнению с традиционными методами, которые занимают много времени и требуют сложного лабораторного анализа, компьютерное зрение было расширено в отрасль искусственного интеллекта (искусственного интеллекта) и имитационной визуализации человека. Он также сочетался с системами освещения, чтобы облегчить получение изображений, продолжающихся с анализом изображений.

Более подробно этапами анализа изображений являются

1) формирование изображения, при котором изображение объекта захватывается и сохраняется в компьютере

2) предварительная обработка изображения, при которой качество изображения улучшается для повышения детализации изображения;

3) сегментация изображения, при которой изображение объекта идентифицируется и отделяется от фона

4) измерение изображения, при котором квантуется несколько значимых признаков;

5) интерпретация изображения, при которой извлеченные изображения затем интерпретируются.

Недавнее развитие технологии обработки изображений дало возможность создать систему распознавания цифрового изображения.

Цифровая обработка изображений или другая обработка изображений, как правило, эволюционируют в наиболее обширный мейнстрим при поддержке других теоретических областей, поддерживаемых быстрым развитием конкретных дисциплин, таких как математика, Линейная алгебра, статистика, вычислительная нейробиология.

Распознавание образов как отрасль компьютерного зрения сосредоточено на процессе идентификации объектов посредством преобразования изображений для получения лучшего качества изображения и интерпретации изображений. Этот процесс направлен на извлечение информации для принятия решений на основе изображений, полученных с датчиков]. Другими словами, компьютерное зрение стремится построить интеллектуальную машину, чтобы "видеть"." Общими фреймворками, используемыми в компьютерном зрении, являются получение изображений, предварительная обработка, извлечение признаков, обнаружение/сегментация, высокоуровневая обработка и принятие решений. Фреймворки компьютерного зрения состояли из двух основных групп, например, 3D-морфологический анализ и пиксельная оптимизация. 3D-морфологический обзор был стандартной теорией для компьютерной обработки изображений и распознавания образов, в то время как пиксельная оптимизация связана с характеристикой морфологии пикселей, включая структурный анализ и внутренние компоненты для лучшего понимания векторной функции. Кроме того, подход должен выполняться на относительно больших наборах данных, охватывающих множество слоев геометрической композиции. Поэтому эффективные и точные вычислительные алгоритмы для извлечения соответствующей количественной информации важны для понимания сложных цветовых кластеров в целом. Интеграция морфологического анализа с некоторыми методами искусственного интеллекта может привести к повышению производительности вычислительных алгоритмов. Вычислительный алгоритм-это нечеткая логика, искусственные нейронные сети и генетические алгоритмы. Их можно комбинировать для полного выполнения сложных задач.

Компьютерное зрение было связано с обработкой изображений и машинным обучением. Компьютерное зрение как область широкого спектра дисциплин было тесно связано с дисциплиной обработки изображений. Обработка изображений сама по себе принесла пользу в различных областях техники, особенно для анализа изображений с целью получения необходимой информации. В качестве технологических областей, которые будут развиваться с помощью компьютерного зрения, он был расширен на другие инженерные

области, такие как географическое дистанционное зондирование, робототехника, компьютерная и человеческая коммуникация, здравоохранение и спутниковая связь. Исследователи, интересующиеся компьютерным зрением, могут использовать эти знания для прогнозирования отдельных событий, анализируя изображения и видео и извлекая их особенности. Поскольку разработки в области компьютерного зрения тесно связаны с обработкой изображений и машинным обучением, его можно использовать в более обширных областях исследований для прогнозирования или обнаружения поведения и характеристик объектов, включая деятельность человека и природные явления.

Список использованных источников

Тимофеев, А.В. Информатика и компьютерный интеллект / А.В. Тимофеев. - М.: Педагогика, 2016. - 128 с.

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИЙ МОНИТОРИНГА В СЕТИ ИНТЕРНЕТ

Уменко Владислав Дмитриевич, курсант 4-го курса
Научный руководитель, Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Мониторинг в наше время является одной из популярных функций в компьютерной разведке. Современная преступность переходит в так называемый статус «Online – преступности», то есть злоумышленники учатся совершать различного рода преступления в Интернете, ведь Интернет является гигантским пространством и “замести” следы в нем бывает очень легко, однако достаточно единожды оставить о себе что-то и это можно будет выявить при правильном поиске, поэтому сотрудники Министерства внутренних дел России занимаются мониторингом, благодаря которому получается найти информацию о преступнике, готовящемся или совершенном преступлении.

В век информационных технологий поиск информации о преступнике либо о готовящемся или совершенном преступлении в некоторых случаях стал намного проще. Мониторинг – это комплекс мероприятий по поиску различной информации в открытых источниках Интернет-пространства, наблюдение за подозрительными личностями, а также слежка за подозрительными сайтами либо блогами в Интернете. Существующие технологии мониторинга сети Интернет нацелены на поиск информации, наблюдение за сайтами, в следствии чего появляются информация, порой даже анкетные данные личности, адрес провайдера.

Одной из технологий мониторинга сети интернет является OSINT (анг. Open source intelligence, OSINT) – разведка на основе открытых источников, целью которой является получение информации из доступных для всех источников. К ним относятся различные ресурсы, доступ к которым имеют абсолютно все. Различные сервисы для коммуникации, то есть социальные сети, сервисы для поиска объектов исследования на основе биометрических данных, поиск информации по геотегам, сервисы с данными о юридических лицах. По критериям поиска открытые технологии можно разделить на: поиск по Ф.И.О.; поиск по номеру телефона; поиск по биометрическим данным; поиск с использованием TelegramBot; поиск по ip (Рисунок – 1).

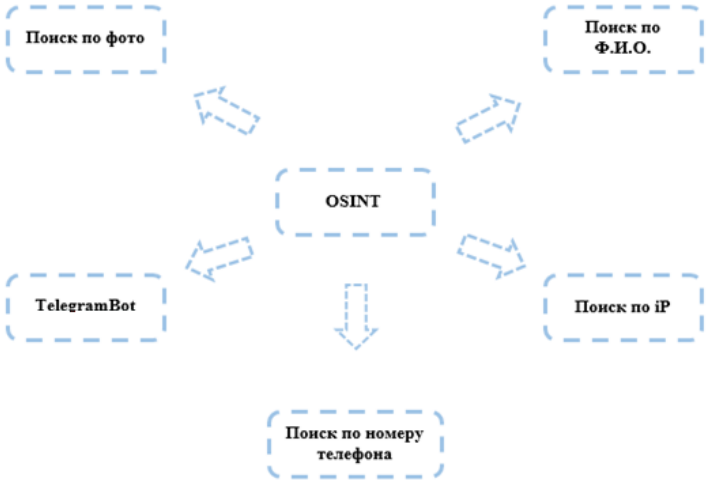


Рисунок – 1 Структура поиска через открытые источники

Представленные способы поиска информации через различные открытые источники можно применять как по отдельности, так и в совокупности. Но, чтобы найти как можно больше информации, нужно применять весь инструментарий OSINT.

К сервисам, позволяющим производить поиск лиц с критерием «фамилия, имя, отчество» относятся различные социальные сети, где пользователи порой выдают о себе много информации, которая сосредоточена на их личности, их образе жизни, членах семьи, домашних питомцах, наличия образования, образа жизни и прочего другого. Каждый фактор, который стал известен в ходе мониторинга социальных сетей позволяет узнать о человеке как можно больше нового, соответственно выстраиваются дальнейшие планы действий по поиску информации уже с помощью других ресурсов. К сервисам, позволяющим находить информацию по критерию Ф.И.О. относятся:

- Социальная сеть vk.com (ВКонтакте);
- Социальная сеть ok.com (Одноклассники);
- Социальная сеть my.mail.ru (Мой мир);
- Телефонный справочник nomer-org.space (Телефонные базы СНГ);

К поиску по биометрическим данным относится FindClone – доступный для всех сервис, позволяющий по биометрическим данным находить клонов и двойников человека с точностью до 0,9% совпадений в социальной сети Вконтакте. Данный сервис существует как интернет-ресурс и как приложение для мобильных ОС Android и iOS. При регистрации можно выполнить 25 бесплатных поисков, но после уже нужно будет платить. Минусом является платные услуги сервиса, ошибка в биометрических данных, предоставление устаревших ссылок на страничку в социальной сети.

В настоящий момент доступным сервисом по поиску информации о владельце номера является приложение для мобильных ОС Android и iOS GetContact. Сервис устроен так: при авторизации в приложении номера телефона анализируется телефонная книга, где все собранные в ней телефонные номера отправляются в базу данных, каждому номеру присущ свой так называемый тег – то есть имя абонента, как он записан у остальных. Так как в сервисе ежедневно авторизуются сотни тысяч новых пользователей, база данных пополняется ежедневно. Минусом является авторизация пользователей. Пользователи, которые ни разу не авторизовались в GetContact не будут иметь так называемых тегов – то есть отсутствие имени у абонента.

В мессенджере Telegram созданы миллионы различных ботов, настроенных на разведку в открытых источниках. У каждого бота подключена своя база данных, которая хранит в себе множество данных о различных личностях, таких как номер телефона, социальные сети, адрес, данные о недвижимости, автомобилях, поиск номера в объявлениях, краткая информация об операторе телефона. Минусом является чрезмерное количество информации, которая не обновляется и соответственно выдает не всегда то, что запрашивают пользователи.

В интернете в свободном доступе существуют множество сайтов, инструментарий которых позволяет определять уникальный идентификатор устройства, подключенного к интернету или Интернет-ресурса, узнать местоположение. Если данный IP-адрес находится на территории Российской Федерации, то МВД России может послать официальный запрос на получение более подробных данных о провайдере.

Данный поиск нацелен чаще всего на мониторинг сайтов, связанных с незаконным оборотом наркотиков, оружия, материалов педофилии и порнографии, экстремистского характера. Минусом данного метода является то, что такие сайты чаще всего зарегистрированы вне Российской Федерации, чаще всего если МВД России посылает запрос на получение данных, им отклоняют в данной случае.

Еще одной технологией мониторинга сети Интернет является наблюдение за различными сайтами, где можно получать конкретную информацию в ходе наблюдения. Такой технологией является парсинг – мониторинг интернет-ресурсов с помощью различных языков программирования. Парсер — это программа, сервис или скрипт, который собирает данные с указанных веб-ресурсов, анализирует их и выдает в нужном формате.

В заключении хочу отметить, что при взаимодействии данных двух технологий можно собрать как можно больше информации, проверить её через различные базы данных, после чего приобщить к уголовному делу. Данные технологии способствуют удаленной и

автоматизированной работе, что упрощает процесс розыска информации о лицах. Поэтому, на современной этапе, мониторинг является одной из важнейших функций в компьютерной разведке. Открытые сервисы, развивающиеся самостоятельно и не имеющие государственной поддержки, за счет бюджета лиц, которые интересуются мониторингом, иногда бывают практически полезны, и информация порой является актуальной и по сей день. Кроме того, нужно отметить, что открытые сервисы предоставляют возможность расширенного поиска необходимых сведений на широких просторах интернета.

Список использованных источников

1. Варлатая, С.К. Защита информационных процессов в компьютерных сетях. Учебно-методический комплекс / С.К. Варлатая. - М.: Проспект, 2017. - 348 с.
2. Дж., Скотт Хогдал Анализ и диагностика компьютерных сетей / Дж. Скотт Хогдал. - М.: ЛОРИ, 2015. - 350 с.

КАК РОССИЯ БУДЕТ ЗАЩИЩАТЬСЯ ОТ УГРОЗ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Фастунов Алексей Дмитриевич, студент 1-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Как Россия будет защищаться от угроз в сфере информационной безопасности:

1) В области обороны:

- будет сдерживать и предотвращать военные конфликты, которые может спровоцировать применение информационных технологий.
- будет совершенствовать систему информационной безопасности армии, причем не только защитного характера, но и атакующие силы («силы и средства информационного противоборства»).
- будет защищать интересы союзников России в информационной сфере.
- будет нейтрализовывать информационно-психологическое воздействие, направленного «на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества».

2) В области государственной и общественной безопасности:

- будет противодействовать пропаганде экстремистской идеологии и средствам ее доставки.
- будет пресекать деятельность спецслужб и организаций иностранных государств, бороться с их техническими средствами.
- будет не допускать иностранный контроль над объектами информационной инфраструктуры.
- будет заниматься профилактикой правонарушений, совершаемых с использованием информационных технологий.
- будет защищать гостайну за счет существующих информационных технологий.
- будет нейтрализовывать информационное воздействие, направленное на размывание традиционных российских духовно-нравственных ценностей.

3) В экономической сфере:

- будет развивать отрасли информационных технологий с помощью поддержки инноваций, будет увеличивать доли этой отрасли в ВВП и структуре экспорта страны.
- будет широко внедрять отечественные разработки.
- будет повышать конкурентоспособность российских компаний, действующих в отрасли информационных технологий.

4) В области науки и образования:

- будет создавать информационные технологии, устойчивые к различным видам внешнего воздействия.
- будет исследовать разрабатывать перспективные технологии и средства обеспечения информационной безопасности.
- будет формировать культуру личной информационной безопасности.

5) В области стратегической стабильности:

- будет проводить самостоятельную политику на реализацию национальных интересов в информационной сфере.
- будет формировать системы международной информационной безопасности с партнерами.

- будет продвигать позиции России на международном уровне, стремиться к взаимовыгодному и равноправному сотрудничеству стран, заинтересованных в информационной сфере.
- будет развивать национальную систему управления российским сегментом сети интернет.

ДЕАНОНИМИЗАЦИЯ ПОЛЬЗОВАТЕЛЕЙ, ИСПОЛЬЗУЮЩИХ TOR

Филимонова Юлия Витальевна, курсант 3-го курса
Научный руководитель, Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

На сегодняшний день сеть Tor является одной из самых больших в мире развернутых анонимных сетей. По статистике, ежемесячное число активных пользователей сети превышает 2 млн. число, а число, используемых в качестве узлов сети, волонтерских серверов превышает 6 тыс.

Наиболее актуальной и важной задачей для специальных служб различных государств является деанонимизация пользователей, так как помимо обычных пользователей преимуществами анонимизации трафика пользуются продавцы оружия и наркотиков, террористы, а также прочие нарушитель закона. Так, например, МВД РФ объявляло тендер на разработку различных способов деанонимизации пользователей сети Tor.

Для того, чтобы организовать атаку, необходимо обладать определенными ресурсами, например, серверами, доступ к которым пытается получить пользователь, или коррумпированными узлами Tor.

Учитывая тот факт, что сеть Tor является оверлейной сетью, стоит отметить, что она работает на основе транспортного слоя. Основными организациями, которые управляют интернет маршрутизацией, являются автономные системы. Атакующий может контролировать одну или несколько автономных систем и предполагается, что он наблюдает трафик, проходящий через автономную систему.

Атакующий, как правило, преследует цель скомпрометировать наибольшее количество цепей, относящихся к конкретному пользователю или группе пользователей, так как компрометирование цепей влечет за собой деанонимизацию пользователей

Учитывая тот факт, что в сети Tor есть спорный контент, например, сайты, продающие наркотики и распространяющие детскую порнографию, правоохранительные органы используют множество методов для деанонимизации некоторых пользователей. Эти методы могут варьироваться от использования человеческого фактора, до сложных математических, которые эксплуатируют недостатки программного обеспечения.

Tor представляет собой службу, которую может запускать сервер или пользователь, это значит, что системы, связанные с сетью Tor, по-прежнему уязвимы для традиционных кибератак. В зависимости от специальных конфигураций системы можно использовать различные методы, чтобы выявить личность веб-пользователя или скрытую службу в сети Tor. Процесс деанонимизации происходит после того, как злоумышленник получает соответствующую информацию или даже полностью контролирует систему, связанную с Tor.

Видимость службы повышает вероятность проведения успешной кибератаки. Типичные атаки на уровне приложений включают обработку сеанса, проверку ввода и контроль доступа, а на уровне операционной системы атаки обычно нацелены на неправильную конфигурацию. Более того, производительность системы может быть подорвана с помощью DDoS-атак, что может привести к сбою системы.

Как правило, атаки проверки ввода основываются на инъекциях и обычно используют переполнение буфера, межсайтовый скриптинг (XSS) и загрузку вредоносных файлов. Атаки обработки сеанса основаны на получении токенов, благодаря которым гарантируется правильное состояние на двух конечных точках связи. Атаки на управление доступом сосредоточены на повышении привилегий, то есть обычный пользователь будет повышен до пользователя с правами администратора.

В августе 2013 года ФБР обнаружило уязвимость в браузере Tor, которую они использовали для атаки сайтов, хостером которых была компания Freedom Hosting. Freedom Hosting отличалась тем, что размещала на своей площадке сайты с детской порнографией. ФБР

удалось получить доступ к серверам Freedom Hosting и внедрить вредоносный код Javascript, который ищет имя хоста и MAC-адрес, а затем передает их обратно как HTTP-запросы на серверы в Вирджинии, таким образом раскрывая реальный IP-адрес пользователя.

Tor не защищен от сквозных атак, основанных на тайминге. Отслеживающий трафик злоумышленник может использовать статистический анализ, чтобы определить, что достигающий первого узла ретрансляции, а затем конечного адресата (скрытая служба) трафик принадлежит к одной и той же схеме. Таким образом, Tor не способствует абсолютной анонимности.

Адрес пользователя, как и адрес назначения отслеживаемого трафика, может получить злоумышленник, который успешно деанонимизирует цель с помощью корреляционных атак. Следует отметить, что злоумышленнику совсем не обязательно иметь полный контроль над первым и последним маршрутизатором в схеме Tor, чтобы иметь возможность коррелировать потоки трафика, контролируемые в этих ретрансляционных узлах. Все, что ему нужно — контролировать трафик.

Иногда деанонимизация не требует выполнения сложных форм статистического анализа. Например, студент Гарвардского университета был арестован за отправку ложных сообщений о минировании через Tor, чтобы выйти с экзамена. Согласно данным ФБР, электронные письма этого студента были отправлены с помощью сервиса Guerilla Mail, позволяющего создавать временные электронные письма.

Guerilla внедряет IP-адрес отправителя во все исходящие письма, и в этом конкретном случае это указывало на IP-адрес выходного узла пользователя Tor. ФБР заявило, что студент отправил электронные письма через Tor из беспроводной сети университета. Корреляция помогла ФБР вычислить студента, который признался во всем во время допроса.

Такие атаки легко осуществить, когда количество клиентов, использующих Tor, относительно невелико. Другими словами, если существует небольшое число людей, использующих Tor, в контексте конкретной сети, то деанонимизировать их относительно несложно.

Более сложные формы атак требуют более сложных методов статистического анализа как трафика, так и тайминга. Недавние исследования показали, что эти методы могут деанонимизировать значительную долю пользователей Tor и скрытых служб.

Список использованных источников

1. Identity theft and protecting personal information. Plymouth Chamber of Commerce: Brown Bag Lunch Series. 2009
2. Romanosky S., l Telang R., Acquisti A. Do Data Breach Disclosure Laws Reduce Identity Theft? / Seventh Workshop on the Economics of Information Security. Hanover. 2008
3. Анин Б.А. Защита компьютерной информации. - СПб.: БХВ-Петербург. 2000.- 384с
4. Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М.: Книжный мир, 2009. – 352 с.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ СТАЛИ ЧАСТЬ ПОВСЕДНЕВНОЙ ЖИЗНИ И В СЛЕДСТВИЕ ПРИОБРЕЛИ ГЛОБАЛЬНЫЙ ХАРАКТЕР

Филюшин Дмитрий Александорович, курсант 1-го курса
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Наиболее характерная черта нынешнего развития мировой экономики — колоссальные успехи и достижения в области техники и технологии, развитие наукоемких производств. Высокие темпы развития науки и технологий, а главное масштабы и темпы их внедрения в производство и общественную жизнь, превратили научно-техническую революцию в естественный процесс, она стала перманентной. Благодаря развитию коммуникаций и росту уровня образования, "ноу-хау" сейчас практически сразу после изобретения становятся общечеловеческим достоянием. В условиях динамичного развития рынка усложнения его инфраструктуры *информация* становится таким же стратегическим ресурсом, как и традиционные материальные и энергетические.

Старая *истина* гласила, что "тот, кто владеет золотом, то владеет миром". Сегодня это не так? миром владеет тот, кто владеет информацией. Но реальную власть дает не сама *информация* как таковая, а умение её извлекать, собирать, анализировать и с пользой применять. А это означает, что важные для бизнеса данные необходимо использовать с целью получения максимальных выгод. И, если получаемые в результате преимущества велики, то это дает все основания считать такую информацию одним из ключевых бизнес-активов предприятия. Если компания будет пренебрегать этими возможностями, то она рискует быстро оказаться на обочине рынка.

Современные технологии, позволяющие создавать, хранить, перерабатывать данные и информацию, обеспечивать эффективные способы представления информации, стали важным фактором конкурентоспособности и средством повышения эффективности управления всеми сферами общественной жизнедеятельности. Уровень информатизации является сегодня одним из главных факторов успешного развития всякого предприятия.

Менеджер любого уровня при принятии решений основывается лишь на доступной ему информации о предмете управления, поэтому от качественных характеристик этой информации таких, как адекватность, полнота, достоверность, своевременность, непротиворечивость и т. п., непосредственно зависит эффективность его работы. В современных условиях информационные технологии и системы играют и будут играть все большую роль и в достижении стратегических целей компаний. Это влечет за собой новые требования к информационным системам и их функциям. Они не могут оставаться просто инструментом, обеспечивающим обработку информации для отделов и конечных пользователей внутри предприятия. Теперь они должны давать новые изделия и услуги, основанные на информации, которые обеспечат бизнесу конкурентное преимущество на рынке.

Используемые на предприятии информационные технологии поддерживают реализацию деловых решений менеджеров. Однако, в свою очередь, новые системы и технологии диктуют свои специфические условия ведения бизнеса, изменяют компании. И каких бы консультантов в этой области руководитель не привлекал, окончательные решения необходимо принимать ему лично. Менеджер должен уметь извлекать максимальную выгоду из потенциальных преимуществ информационных технологий. Он обязан обладать достаточными знаниями для того, чтобы осуществлять общее руководство процессом применения и развития информационных технологий в компании и понимать, когда

требуются дополнительные затраты ресурсов в этой области или помощь сторонних специалистов.

Основная цель этого курса — дать общее системное представление об информации, методах ее хранения, обработки и передачи, о современных информационных технологиях и системах, истории их развития, влиянии на общество и бизнес, методологиях их применения в деятельности предприятия. Поскольку каждая из рассматриваемых в курсе тем представляет собой достаточно большую и самостоятельную предметную область применения современных информационных технологий в управлении бизнесом и информационного менеджмента, то разные темы курса можно рассматривать как вводные в соответствующие дисциплины.

1. Развитие информационных технологий

Информационные технологии (ИТ) являются наиболее важной составляющей процесса использования информационных ресурсов общества. К настоящему времени ИТ прошли несколько эволюционных этапов, смена которых определялась главным образом техническим прогрессом, появлением новых технологических средств поиска и переработки данных. Последний по времени этап, часто называемый новым, характеризуется изменением направленности ИТ с развития технических средств на создания стратегического преимущества в бизнесе.

1.1. Предпосылки быстрого развития информационных технологий

До недавнего времени информация не считалась важнейшим активом для компании. Процесс управления деятельностью организации в большой степени зависел от персонального воздействия первых лиц компаний без обширного процесса координации усилий менеджеров и анализа данных. Деловые решения принимались первыми лицами компаний чаще всего на основе опыта и интуиции, и лишь в небольшом числе случаев — на основе специально подготовленной информации, содержащей варианты решений и оценку вероятности их осуществимости. Лишь мощные компании могли позволить себе иметь аналитические центры, готовившие материал для принятия решений. Развитие вычислительной техники кардинально изменило окружающую среду бизнеса. На рис. 1.1 показаны главные предпосылки развития ИТ, основанные на компьютерных и телекоммуникационных технологиях.

Рис. 1.1. Предпосылки развития ИТ

Глобализация и интегрированное развитие индустриальных экономик значительно расширяет возможности бизнеса. Информационные технологии и информационные системы (ИТ/ИС) обеспечивают мобильный доступ и аналитическую мощь, которые удовлетворяют потребности в проведении торговли и руководстве предприятиями в масштабе стран и

континентов. Это создает угрозы национальным и региональным фирмам: глобальная связь и системы управления доставляют потребителю информацию о предложениях, качестве и ценах и позволяют совершать сделки и заказы в течение 24 часов в сутки в любом месте, где есть доступ в сеть.

В таблице 1.1 приведены основополагающие факторы, необратимо изменившие к концу XX века деловую среду.

Таблица 1.1.

Глобализация	**Преобразование индустриальных экономик**	**Преобразование предприятия**
Управление и контроль в глобальном масштабе Конкуренция и взаимодействие на мировых рынках Глобальные системы доставки информации Распределенная групповая работа Международные соглашения и стандарты	Экономика, основанная на знаниях и информации Стратегические ценность информации Знания как основа производительности и качества Новые изделия и услуги Конкуренция, основанная на скорости принятия оптимального решения Расширение базы знаний персонала	Неформальные цели и обязательства Децентрализация и гибкость Локальная независимость Расширение полномочий Снижение стоимости сделок за счет информационного маркетинга Смещение фокуса с технологии на потребителя

Таким образом, мировой рынок становится открытым, ни одна из фирм не может чувствовать себя в безопасности. Чтобы стать эффективным участником этого рынка, компании нуждаются в мощной информационной поддержке и современных системах связи.

1.2. Этапы развития информационных технологий

Существует несколько возможностей классификации развития ИТ с использованием компьютеров, которые определяются различными качественными признаками деления на этапы. Основной целью применения ИТ становится удовлетворение корпоративных и персональных информационных потребностей. Ниже приводится несколько таких классификаций.

Проблемы, стоящие на пути информатизации общества

Современный этап развития современных информационных технологий, начавшийся с начала 90-х годов, характеризуется созданием больших ИС, локальных, региональных и глобальных сетей. Проблемы этого этапа весьма многочисленны. Наиболее существенными из них являются:

- выработка соглашений и установление стандартов, протоколов для компьютерных разработок и телекоммуникаций;
- необходимость разработки распределенных ИС;
- организация доступа к стратегической информации;
- организация защиты и безопасности корпоративной информации.

Задачи и процессы обработки информации

Задачи обработки информации на современном этапе состоят в создании ИТ, направленных на решение стратегических задач, и реализацию информационных систем управления процессами (ИСУП) и поддержки принятия делового решения (ИСППР).

Преимущества применения компьютерных технологий

Преимущества применения компьютерных технологий на современном этапе связаны с появлением персональных компьютеров. Изменился подход к созданию ИС — ориентация смещается в сторону индивидуального пользователя для поддержки принимаемых им решений. Пользователь заинтересован в проводимой разработке, налаживается контакт с разработчиком, возникает взаимопонимание обеих групп специалистов. На этом этапе используются как централизованная обработка данных, характерная для первого этапа, так и децентрализованная, базирующаяся на решении локальных задач и работе с локальными базами данных на рабочем месте пользователя.

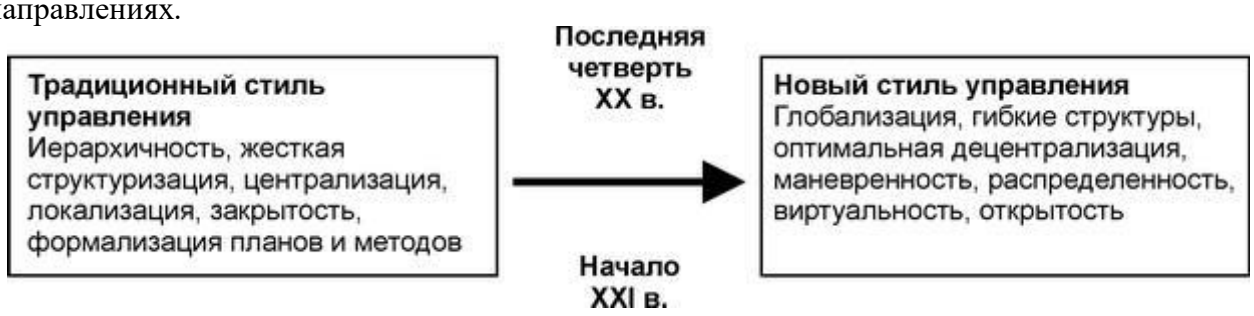
Преимущества применения компьютерных технологий на современном этапе связаны с той ролью, которую они играют в бизнесе, и основаны на достижениях телекоммуникационных технологий и распределённой обработке информации. ИС имеют своей целью не просто увеличение эффективности обработки данных и помощь управленцу, а создание высокоэффективного производства. Применяемые ИТ должны помочь компании выстоять в конкурентной борьбе и получить преимущество.

Инструментальные технологические средства

Основными инструментальными технологическими средствами современного этапа развития ИТ стали "Internet/Intranet (новейшие)" технологии. Широко используются в различных областях науки, техники и бизнеса распределенные системы, глобальные, региональные и локальные компьютерные сети. Развивается электронная коммерция. В связи с переходом на микропроцессорную базу существенным изменением подвергаются технические средства связи, средства бытового, культурного и прочего назначений.

1.3. Тенденции развития ИТ

При традиционном подходе к организации, когда специализированные функции включаются в дело одна за другой, как в эстафете, высокая эффективность недостижима. Быстрота реагирования на внешние изменения требует постоянного сотрудничества между разными специализированными отделами и службами. Постоянно общаясь и обмениваясь информацией, они могут действовать быстро, согласованно и одновременно в самых разных направлениях.



ТЕХНИЧЕСКИЕ МЕРЫ ПРЕДОСТОРОЖНОСТИ ДЛЯ ЗАЩИТЫ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Фролкина Алина Михайловна, курсант 3-го курса
Научный руководитель, Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Защита устройств от вредоносного программного обеспечения

Информационно-телекоммуникационные системы постоянно подвергаются определенным угрозам, а неправильное использование может нанести значительный ущерб компаниям и потребителям. Одна из угроз исходит от различных типов вредоносных программ, которые могут быть использованы, например, для попадания конфиденциальной информации в неавторизованные руки или для повреждения используемых ИТ-систем.

Чтобы предотвратить заражение таких устройств, как ПК, ноутбуки, смартфоны или других ИТ-систем вредоносным ПО, в первую очередь, необходимо принять различные меры для обеспечения максимально возможной защиты. Для этого необходимо сначала выработать некоторые общие меры безопасности. Однако одного этого пункта будет недостаточно. Поэтому необходимо принять дополнительные меры против социального взлома, чтобы быть как можно более уверенным в своей безопасности.

Кроме того, необходимо принимать технические меры предосторожности для защиты ИТ-систем от всех видов вредоносного ПО. Так как цепь прочна только как самое слабое звено, необходимо позаботиться о том, чтобы разработанные меры осуществлялись последовательно в любое время и в любом месте. Необходимые меры зависят от используемых IT-систем и личных обстоятельств. Поэтому следующие пункты являются только примерами и должны быть разработаны индивидуально.

Антивирусная программа

Наиболее важным базовым оборудованием на каждом используемом устройстве, включая смартфоны или ноутбуки, является хорошая антивирусная программа. Здесь следует обращать внимание не на цену, а на то, что антивирусная программа хороша и своевременно обнаруживает известные и неизвестные вредоносные программы. Она должна обеспечивать комплексную защиту от всех видов вредоносного ПО и детектировать новейшие технологии, используемые хакерами.

Обновление антивирусной программы

В связи с тем, что новые вредоносные программы постоянно программируются и распространяются, антивирусные программы должны постоянно обновляться через Интернет, чтобы максимально защитить устройства от новейших известных угроз. Запуск обновлений осуществляется либо вручную, либо антивирусная программа обновляет себя через определенные промежутки времени, желательно ежедневно.

Обновление операционной системы и программ

То, что относится к антивирусной программе, относится также к операционной системе, ко всем установленным программам и драйверам, необходимым для аппаратного обеспечения. Необходимо всегда держать их в курсе и, прежде всего, устанавливать доступные обновления безопасности, предоставляемые производителями. По возможности загружать их только непосредственно у соответствующего производителя или, по крайней мере, убедиться в том, что источники загрузки абсолютно надежны и заслуживают доверия.

Сканирование всех дисков на наличие угроз

Антивирусные программы обычно предлагают возможность проверки всех носителей данных на наличие вредоносных программ. Через определенные промежутки нужно сканировать все носители данных. Особенно, если возникают подозрительные действия, например, внезапная поломка компьютера.

Брандмауэр

IT-системы общаются друг с другом различными способами, например, когда локальный компьютер вызывает веб-сайт, он общается с сервером в Интернете, на котором хранится веб-сайт. Для связи используются различные каналы, например, для отправки и получения команд управления или пакетов данных. Эти каналы также называются портами. Хакеры могут использовать открытые порты для всех видов атак.

Для предотвращения неконтролируемой связи через открытые порты все устройства должны быть оснащены брандмауэром. Они действуют как фильтр, контролируя доступ к системе и из системы и, например, разрешая доступ только тем, кто разрешен в соответствии с правилами, установленными в настройках брандмауэра. Определение правил очень важно, и с их помощью можно сделать множество различных настроек. Например, можно разрешить доступ к порту только на определенные IP-адреса или с них. Также можно установить различные правила для входящего и исходящего доступа через порт. Например, разрешить исходящий доступ, но заблокировать входящий доступ.

Брандмауэры делятся на аппаратные и программные. В компаниях в основном используются аппаратные брандмауэры. Это специальные устройства, которые также содержат программное обеспечение и используются для управления трафиком данных. Кроме того, часто используются программные брандмауэры, которые работают на специально настроенных компьютерах. Такие решения, как правило, слишком дороги для домашних пользователей, поэтому для этой целевой группы предлагаются так называемые персональные брандмауэры. В основном это программные брандмауэры, которые устанавливаются и настраиваются на домашних компьютерах, как обычные программы.

Защита маршрутизатора/модема

Каждый компьютер подключается к Интернету через модем или маршрутизатор. Поэтому они являются первой возможной точкой атаки и должны быть максимально защищены. Например, всегда следует запускать маршрутизатор с последней прошивкой, содержащей последние исправления безопасности. Кроме того, все пароли по умолчанию должны быть заменены собственными безопасными паролями. Это связано с тем, что маршрутизаторы часто имеют пароли заводской установки, которые можно взять из руководств, например 1234 или 0000. Если эти пароли заводской установки не будут изменены, то теоретически любой может получить доступ к маршрутизатору, а также манипулировать им или использовать его в других ненадлежащих целях.

Одной из возможностей является замена DNS-серверов в маршрутизаторе и направление пользователей на поддельные веб-сайты. Это очень опасно, так как обнаружение подделки этим методом чрезвычайно затруднено, и если это хорошо сделано, то подделка может вообще не быть обнаружена. Потому что, по сути, можно настроить веб-страницу с любым интернет-адресом на любом веб-сервере в Интернете. Посетители обычно не попадают на эти поддельные веб-серверы, потому что DNS-серверы направляют их на нужный веб-сервер. Однако, если манипулировать настройками DNS, это может иметь фатальные последствия, если, например, пользователь думаете, что находится на сайте банка и вводите PIN-коды и TAN-коды на поддельном сайте. Преступники могут использовать это, например, для осуществления банковского перевода.

Переключение просмотра электронной почты на обычный текст

В почтовых программах существуют различные режимы просмотра для чтения писем, например, HTML, RTF или простого текста. Настройка HTML приводит к тому, что письмо отображается более или менее похоже на веб-страницу. Это может привести к проблемам. Например, файлы могут быть встроены в веб-страницы. Некоторые люди используют эту возможность для встраивания подготовленных файлов, с помощью которых можно использовать дыры в безопасности и загружать вредоносное ПО. Настройка RTF также не является абсолютно безопасной, так как стали известны возможности проникновения вредоносных программ. Коварство настройки HTML или RTF заключается в том, что вредоносная программа может быть внедрена без открытия вложения файла. Достаточно просто просмотреть электронное письмо, например, в окне предварительного просмотра,

который задается во многих почтовых программах. Поэтому, из соображений безопасности, вид в почтовых программах должен быть изменен на текстовый.

В текстовом представлении форматирование писем теряется, и они могут быть некрасивыми, но более безопасными. У него есть и другие преимущества. Например, многие хакеры скрывают цели ссылок в сообщениях электронной почты за изображениями, которые действуют как кнопки. Многие из них также включают изображения в сообщениях электронной почты, которые автоматически загружаются с других серверов, просто для того, чтобы определить, существует ли адрес электронной почты и прочитал ли получатель это сообщение. В текстовом представлении изображения не отображаются, поэтому их больше нельзя использовать для таких целей. Это, в дополнение к повышению безопасности, на самом деле может привести к сокращению количества спам-сообщений, которые многие люди получают ежедневно.

Не использовать учетную запись администратора

В рамках настройки операционной системы на компьютере создается учетная запись администратора. С помощью этой учетной записи пользователя можно войти на компьютер и иметь полные права доступа к нему. Вы можете использовать учетную запись администратора для изменения настроек безопасности, установки и удаления программ, настройки или изменения других учетных записей пользователей, а также доступа ко всем файлам. Для обычной деятельности не следует по возможности работать с учетной записью администратора, так как это связано с определенным риском безопасности. Если, например, вредоносная программа контрабандно ввозится и исполняется, то это делается с правами зарегистрированного пользователя. В таком случае весь компьютер будет полностью незащищён администраторской учётной записью, и практически все мыслимые действия возможны.

Поэтому для нормальной деятельности необходимо создать и работать с учетной записью пользователя с ограниченными правами. В качестве дополнительной меры безопасности, учетная запись администратора должна быть деактивирована, защищена надежным паролем. Однако в этом отношении следует проявлять осторожность. Вы должны знать, как при необходимости реактивировать счет. В противном случае может случиться, что администратор практически блокируется, и никаких изменений в систему вносить нельзя.

Отделить личные файлы от системы

Когда пользователь использует компьютер, он имеете дело с операционной системой, программами и личными файлами. По возможности персональные файлы должны находиться не на том же жестком диске, на котором установлена операционная система, а на отдельном. Лучше всего хранить их на внешнем жестком диске, который обычно выключается и включается только при необходимости. В случае атаки вредоносного ПО эти данные будут в некоторой степени защищены.

Меры в случае атаки вредоносного ПО

Если компьютер, несмотря на все меры защиты, заражен вредоносным ПО, следует, с одной стороны, стараться минимизировать ущерб, а с другой - как можно быстрее удалять вредоносное ПО. Кроме того, необходимо принять меры, чтобы, по крайней мере, создать резервную копию важных данных. После заражения носители данных, такие как жесткие диски или USB-флешки, по возможности, не следует повторно использовать, так как они представляют постоянную опасность. Например, вполне возможно, что вредоносная программа укоренится настолько, что даже переживет форматирование.

Заражен ли компьютер вредоносным ПО или нет, к сожалению, не всегда можно четко определить. Частыми признаками заражения вредоносным ПО являются определенные аномалии, например, когда программы больше не запускаются должным образом или аварийно завершаются.

Список использованных источников

1. Гордеев, Александр Владимирович. Операционные системы [Текст] : учеб. для вузов по направлению подгот. бакалавров и магистров «Информатика и вычисл. Техника» и направлению подгот. дипломир. специалистов «Информатика и вычисл. Техника» / А. В. Гордеев. - 2-е изд. - СПб.: Питер: Питер принт, 2005. - 415 с.
2. Олифер, Виктор Григорьевич. Сетевые операционные системы [Текст] : учеб. пособие для вузов по направлению подгот. дипломир. специалистов «Информатика и вычисл. техника» / В. Г. Олифер, Н. А. Олифер. - СПб.: Питер: Питер Пресс, 2007. - 538 с.
3. Столлингс, Вильям. Операционные системы [Текст] :внутрен. устройство и принципы проектирования / Вильям Столлингс; пер. с англ. - М. [и др.] : Вильямс, 2004. - 843 с.
4. Бэкон, Джин. Операционные системы [Текст] : парал. и распре дел. системы / Джин Бэкон, Тим Харрис; пер. с англ. - СПб.: Питер, 2004. - 799 с.
5. Таненбаум, Эндрю. Современные операционные системы [Текст] / Э. Таненбаум. - 2-е изд., перераб. и испр. - СПб.: Питер: Питер Пресс, 2007. - 1037 с. - (Классика computer science).

ПРИМЕНЕНИЕ ДВУХФАКТОРНОЙ АУТЕНТИФИКАЦИИ

Фролов Дмитрий Сергеевич, курсант 3-го курса
Научный руководитель, Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Г. Москва

Актуальность темы заключается в том, что на сегодняшний момент необходимы качественные и надежные средства защиты, позволяющие смело хранить разного количества объема личных данных, сбережений на собственном виртуальном аккаунте, при этом не беспокоясь за их конфиденциальность и сохранность.

Главная тенденция развития современного общества тесно связана с ростом информационной безопасности (ИБ). Приоритетными на современном этапе рассматриваются вопросы ИБ.

Современные технологии постоянно совершенствуются, поэтому такими основами жизни, как безопасность, не следует пренебрегать.

Известно, что более 25 % злоупотреблений информацией в информационных системах (ИС) совершаются внутренними партнерами, пользователями и поставщиками услуг, обладающими доступом к информационным системам. 64% из них – это кража информации, а 21% - финансовое мошенничество. Все это становится возможным из-за несовершенства технологий аутентификации пользователей ИС и разграничения доступа. Одним из приоритетов развития информационных систем является совершенствование управления доступом и регистрация пользователей.

На данный момент в автоматизированных системах присутствует разнообразие средств и методов защиты информации, что наглядно отражает многообразие возможных способов несанкционированных действий.

В настоящее время информационные технологии (ИТ) имеют важнейшее значение во многих сферах деятельности. Все труднее становится представить обычный рабочий день без взаимодействия с интернетом. ИТ стали неотъемлемой частью государственного управления, бизнеса, развлечений и т.д. Появляется огромное количество ресурсов, соответственно, требующие необходимую защиту личных данных. В связи с достижением такого результата, что логично, возникают неприятели, которые не прочь нажиться на халатности, ошибках и слабостях владельцев аккаунтов информационных устройств. А для того, чтобы предотвратить мошеннические действия нужна защита, с помощью которой можно будет пресечь утечку информации.

Аутентификация и является собой прекрасный пример создания механизма защиты личных данных. Она представляет собой процедуру установления подлинности или соответствия.

Многофакторная аутентификация, как ее по-другому называют, - это два уровня защиты. Как часто бывает, первый уровень – логин и пароль. В качестве второго уровня выступают различные средства защиты:

- Одноразовые пароли (почта или SMS) - это проверочный код, необходимый для подтверждения подлинности.
- Телефонный звонок.
- Токены - компактное устройство, предназначенное для обеспечения информационной безопасности пользователя.
- Биометрические данные - сравнение и обзор методов проверки.
- Приложения-аутентификаторы.
- Резервные ключи.

Использование той или иной формы двухфакторной аутентификации значительно затрудняет злоумышленникам взлом учетной записи, обеспечивая безопасность компании и данных клиентов.

Необходимость применения данного способа защиты пользователей от несанкционированного доступа возникла у многих сайтов и ресурсов глобальной сети интернет. Вот, например, небольшой перечень порталов для которых это не просто атрибут в настройках, а некоторый ключевой элемент, который может в существенной степени повлиять на безопасность учетной записи: «Яндекс», «ВКонтакте», «Facebook», «Google», «Twitter», «Instagram».

Сейчас у каждой уважаемой себя компании или организации, которая осуществляется деятельность во всемирной паутине и, где есть возможность регистрировать аккаунт - должна быть функция двухфакторной аутентификации. Здесь даже дело не в уважении, а в требовании к безопасности в современном мире. Пароль и ПИН-код при наличии времени и ресурсов подбирается за крайне малый промежуток времени, в то время, как получить второй фактор не всегда представляется возможным для преступника. Именно, поэтому наличие данной функции можно наблюдать практически на каждом сервисе или сайте (где есть учетные записи пользователей.

В данной теме было рассмотрено применение двухэтапной аутентификации. Это является еще одним плюсом при оценивании его полезности, так как в случае отсутствия интернета можно воспользоваться способом, не требующим подключения интернет соединения.

Подводя итог, можно сказать, что двухфакторная аутентификация стала практически необходимой частью процесса входа в аккаунт. Именно этот способ добавил уверенности не возникновения утечки личных данных, а также надежности его применения.

Также необходимо заметить присутствие настоящего метода аутентификации на большом количестве известных ресурсах страны.

Двухфакторная аутентификация обладает, хоть и в маленькой степени, уязвимостями, но при умелом и качественном подходе к защите собственных данных этого можно избежать.

Данный способ не обязательно активировать повсеместно, где только заблагорассудится. Достаточно лишь защитить аккаунты, в которых хранятся конфиденциальная информация, денежные средства и пароли.

Список использованных источников

1. Головко, Н. Системы и методы аутентификации пользователей [Электронный ресурс]. / Н. Головко. – Режим доступа: https://www.anti-malware.ru/analytics/Technology_Analysis/overview-of-user-authentication-systems-and-methods#part3
2. Двухфакторная аутентификация [Электронный ресурс]. / – Режим доступа: http://withsecurity.ru/chto-takoe-dvuhfaktornaya-autentifikaciya
3. Донохью Б. Двухфакторная аутентификация: что это и зачем оно нужно? [Электронный ресурс]. / Б. Донохью. – Режим доступа: https://www.kaspersky.ru/blog/2fa-practical-guide/21495/
4. Козориз, А. 5 способов двухфакторной аутентификации, их преимущества и недостатки [Электронный ресурс]. / А. Козориз. – Режим доступа: https://lifehacker.ru/two-factor-authentication/
5. Родичев Ю.А. Нормативная база и стандарты в области информационной безопасности / Родичев Ю.А. – М.: Питер, 2017. – 550 с.
6. Шелупанова, А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / Шелупанова А.А., Груздева С.Л., Нахаева Ю.С. – М.: Горячая линия-Телеком, 2015. – 256 с.

VOIP КАК СРЕДСТВО ПЕРЕДАЧИ ГОЛОСА

Хорзова Ирина Сергеевна, 4 курс ФПСОИБ
Научный руководитель Казанцев Владимир Иванович преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

Обсуждение информационно телекоммуникационных технологий (ИКТ) также может быть неполным без обсуждения использования VoIP для инноваций в области телекоммуникаций. Voice over IP заменяет традиционную проводную связь для передачи голоса. Все чаще пользователи могут использовать настольные телефоны или другие конечные точки для голосового вызова через Интернет, а не по традиционным стационарным телефонам или даже более современным каналам сотовой телефонии.

Здесь ИКТ могут быть поучительными. Эти типы сетей ИКТ могут включать в себя также унификацию обмена сообщениями и социальных структур.

В качестве дополнительного примера некоторые структуры ИКТ могут иметь другие инфраструктурные цели, такие как снижение затрат на передачу связи и унификация каналов. Все это может жить под знаменем ИКТ, поскольку мы продвигаемся вперед с такими инновациями, как UC, виртуализация, искусственный интеллект и Интернет вещей, который требует более развитых сетевых систем. ИКТ будут представлять собой ту категорию, которая касается современных коммуникаций в каждую новую эпоху.

VoIP-телефония — технология, совершившая революцию в связи, поскольку она позволила передавать голосовые сообщения через интернет-протоколы. Ее название так и расшифровывается: «Voice over Internet Protocol» — «голос через интернет-протокол». В общем случае под VoIP подразумеваются все способы передачи голоса по IP-каналам, в том числе и такие не относящиеся к телефонии вещи, как срабатывание оповещений или работа наблюдательных систем. Но сейчас речь пойдет о конкретном применении этой технологии, с которой сталкивается большинство из нас — IP-телефонии.

С помощью IP-телефонии можно звонить не только на устройства, подключенные к сети, но и на обычные стационарные и мобильные телефоны. Для этого используются специальные шлюзы, размещенные по всему миру. При выполнении звонка через систему IP-телефонии голос преобразуется в пакет данных с помощью специального кодека. Данные пересылаются через IP-сети, то есть, через Интернет, к получателю, где декодируются в голосовой сигнал. В отличие от обычной телефонной сети, пользователь с присвоенным ему определенным номером может находиться где угодно, лишь бы в месте, где он сейчас оказался, имелся Интернет и оборудование для звонков. Причем в качестве такого оборудования достаточно ноутбука и даже смартфона.

Отсюда вытекает важное преимущество VoIP. В традиционной телефонии стоимость связи увеличивается с расстоянием между абонентами. В IP-телефонии нет никакой разницы, в какой точке мира находятся адреса, между которыми надо передать пакеты данных, лишь бы они были доступны: зашли на сервер IP-телефонии под своим логином и паролем и разговаривайте столько, сколько нужно, независимо от того, где сейчас находитесь. Это дает еще одно важное преимущество — междугородние и международные звонки становятся значительно дешевле.

Для связи с абонентами с помощью IP-телефонии можно использовать следующие варианты:

- IP-телефоны;
- обычные телефоны с проводной или радиотрубкой;
- программные ip-телефоны или софтфоны.

Выбор конкретной конфигурации оборудования для IP-телефонии зависит от бюджета и решаемых задач.

Выбор конкретной конфигурации оборудования для IP-телефонии зависит от бюджета и решаемых задач. К примеру, если работа связана с разъездами, предпочтительно использовать мобильные телефоны. Для организации колл-центров в условиях ограниченного бюджета используют софтфоны, установленные на десктопы. В тех случаях, когда нужна стабильная, качественная и удобная связь, лучше выбрать IP-телефон с проводной или радиотрубкой или подключить обычный аналоговый телефон через VoIP-шлюз.

Настройка подключения к поставщикам услуг IP-телефонии, в целом, схожа у всех операторов. Для подключения необходимо прописать в IP-телефонах, VoIP-шлюзах и софтфонах адреса серверов и ваши идентификационные номера в сети в соответствии с инструкциями конкретного поставщика услуг. После подключения можно начинать звонить клиентам, коллегам, партнерам и заказчикам.

ИССЛЕДОВАНИЕ ЗАВИСИМОСТИ СИЛ РЕЗАНИЯ ОТ УГЛОВ ЗАТОЧКИ РЕЗЦА ПРИ ПОМОЩИ КОМПЬЮТЕРНОГО МОДЕЛИРОВАНИЯ

Хорошилова Наталья Олеговна, студентка 4-го курса
Научный руководитель Маслов Игорь Владимирович, преподаватель
Старооскольский технологический институт им. А. А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В данной работе проведем исследование зависимости сил резания от углов заточки резца при помощи компьютерного моделирования, нам понадобятся исходные данные.

На токарно-винторезном станке 16К20 подрезается торец диаметром D = 120 мм до диаметра d = 80 мм, длина детали l =240 мм. Припуск на обработку h = 2 мм. Параметр шероховатости обработанной поверхности Rz = 20 мкм. Материал заготовки – серый чугун СЧ 20 твердостью 210 НВ. Заготовка предварительно обработана. Система станок – приспособление – инструмент – деталь жесткая.

Выбираем токарный проходной резец отогнутый правый. Материал режущей части – твердый сплав ВК6; сечение корпуса резца 16×25 мм. Форма передней поверхности лезвия – плоская с фаской; геометрические элементы лезвия: передний угол $\gamma = 15°$; задний угол $\alpha = 10°$; угол наклона лезвия $\lambda = 0°$; главный угол в плане $\varphi = 45°$; вспомогательный угол в плане $\varphi_1 = 45°$; радиус вершины r = 1.

Назначаем режим резания [1]. Устанавливаем глубину резания, при снятии припуска за один проход t = h = 2 мм. Назначаем подачу. Для параметра шероховатости поверхности $R_z = 20$ мкм при обработке чугуна резцом с r = 1 мм рекомендуется $S_o = 0{,}25 - 0{,}40$ мм/об. Принимаем среднее значение $S_o = 0{,}38$ мм/об, корректируем по паспорту станка, устанавливаем $S_o = 0{,}35$ мм/об.

Вставляем заданные параметры в компьютерную модель.

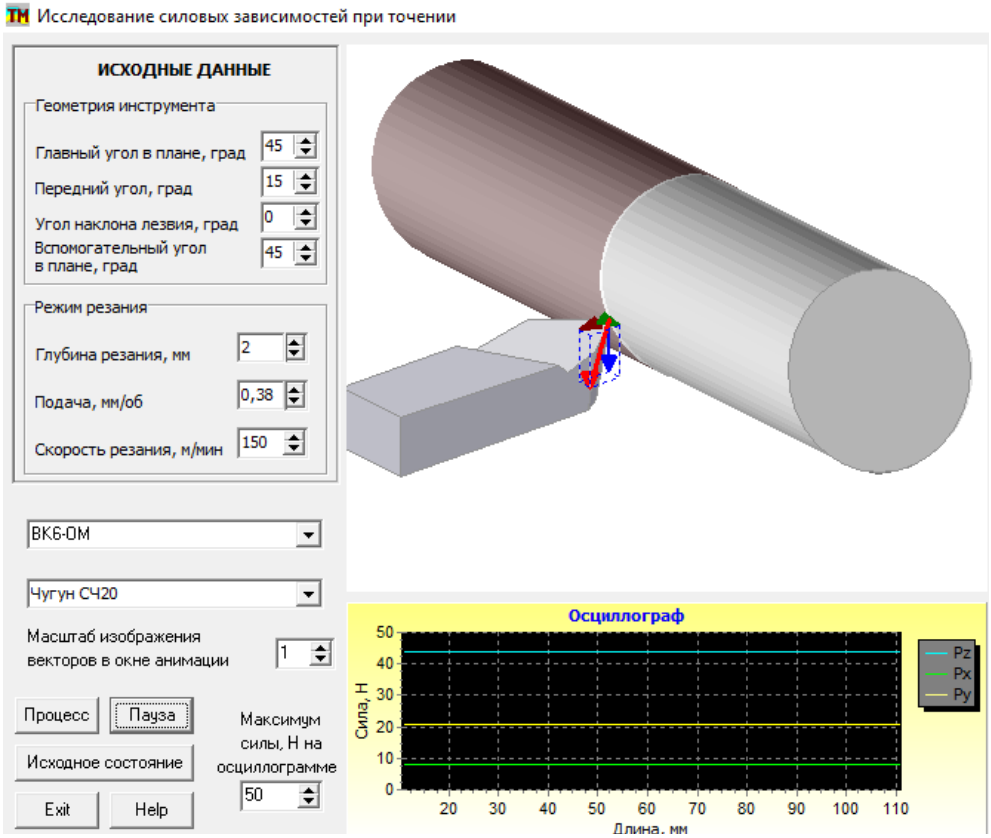


Рисунок 1. Исходные данные

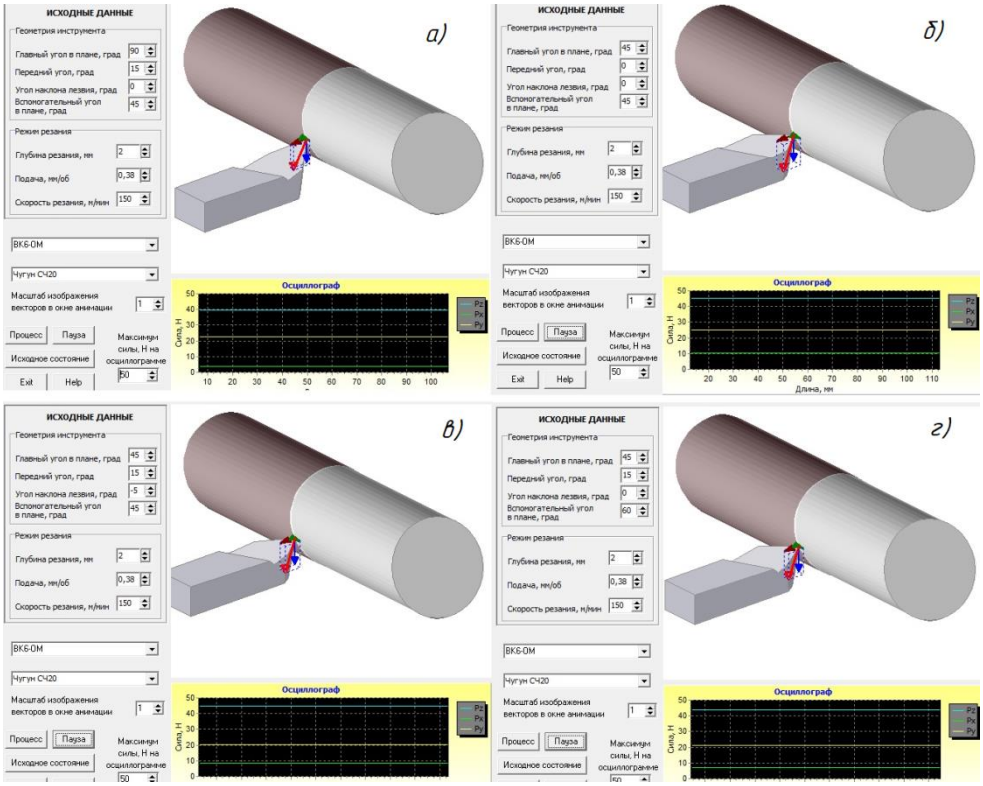


Рисунок 2. Измененные данные

Запускаем процесс, поочередно изменяя углы резца, оставляя неизменными остальные параметры резания.

В исходном состоянии силы резания равны Pz = 43 Н, Py = 21 Н, Px = 8 Н (рисунок 1)

Изменив главный угол в плане с 45° до 90° (рисунок 2, а) получаем:

Pz = 40 Н, Py = 22 Н, Px = 4 Н.

Делаем вывод, что увеличение главного угла в плане приводит к повышению сил Pz и Py и к понижению силы Px.

Изменив передний угол с 15° до 0° (рисунок 2, б) получаем:

Pz = 45 Н, Py = 25 Н, Px = 10 Н.

Делаем вывод, что уменьшение переднего угла приводит к повышению сил Pz, Py и Px.

Изменив угол наклона лезвия с 0° до -5° (рисунок 2, в) получаем:

Pz = 45 Н, Py = 20 Н, Px = 9 Н.

Делаем вывод, что уменьшение угла наклона лезвия приводит к повышению сил Pz и Px и к понижению силы Py.

Изменив вспомогательный угол в плане с 45° до 60° (рисунок 2, г) получаем:

Pz = 44 Н, Py = 21 Н, Px = 7 Н.

Делаем вывод, что увеличение вспомогательного угла в плане приводит к повышению силы Pz, понижению силы Px и не влияет на силу Py.

Таким образом, используя компьютерное моделирование «Исследование силовых зависимостей при точении» [2], мы наглядно определили зависимости сил резания от углов заточки резца.

Список использованных источников

1. Климов И.М. Учебное пособие к выполнению практических и лабораторных работ, курсового и дипломного проектирования – Старый Оскол : СТИ НИТУ МИСиС, 2017.-186 с.

2. Петраков Ю. В. Моделирование процессов резания: учебное пособие для студентов высших учебных заведений/ Ю.В. Петраков, О.И. Драчёв. - Старый Оскол: ТНТ, 2011. - 239 с.

ТРЕКИНГ-КОНТРОЛЬ СОТОВОГО ТЕЛЕФОНА НА БАЗЕ ОС ANDROID

Черкесова Дарья Александровна, курсант 3-го курса
Научный руководитель Толстых Андрей Андреевич, преподаватель
Федеральное государственное казенное образовательное учреждение высшего образования
«Московский университет Министерства внутренних дел Российской Федерации
имени В.Я. Кикотя», г. Москва

В современном мире можно сказать, что каждый человек является владельцем мобильного устройства или каким-то образом связан с информационным пространством. Сотовые телефоны стали неотъемлемой частью жизни человека. Существуют множество ОС для сотовых телефонов, но наиболее доступной на сегодняшний день является продукция на базе ОС Android. На конференции разработчиков I/O 2019 Google заявила, что всего насчитывается 2,5 млрд. действующих Android-устройств, что делает его самой распространённой операционной системой по числу пользователей. В 2020 году тематика трекингконтроля сотовых телефонов стала особенно необходимой, так в России Минкомсвяз и разработало правило отслеживания контактов пациентов больных COVID-19, получив номер телефона заболевшего от Минздрава, власти могли производить мониторинг, и отслеживать геолокацию заразившегося, и вместе с этим составлялся перечень тех, кто находился рядом с заболевшим. Делалось это на основе геолокации заболевшего и данных операторов связи, в результате чего список абонентов, подверженных риску заражения COVID-19 при прямом контакте с пациентом, концентрируется на информационных ресурсах Минкомсвязи и отправляется в оперативные штабы субъектов Российской Федерации, МВД и Минздрава.

Если говорить о трекинг-контроле, то нужно чётко понимать, когда он будет осуществлён, и какие цели будет преследовать. Одно дело, если трекинг-контроль будет осуществлён, как метод наблюдения за работниками в рабочее время, и совсем другое, когда человек в не рабочее время не знает, что за ним ведётся слежка, и тут уже затрагивается частная жизнь человека, которая защищается Конституцией РФ. Конституция Российской Федерации четко определяет права и свободы гражданина, в том числе неприкосновенность его личной жизни. Статья 24 Конституции Российской Федерации запрещает использование сведений о частной жизни человека.

Чтобы ответить на вопрос о правомерности отслеживания мобильного телефона, нужно понимать, при каких обстоятельствах и в каких целях производится трекинг-контроль сотового телефона. Помимо этого, стоит обратиться к установленному законодательством толкованию термина «частная жизнь»: это только та информация, которая касается исключительно данного человека и не подлежит стороннему контролю или контролю государства.

По сути, трекинг-контроль сотового телефона сотрудника в рабочее время – это отслеживание мобильного телефона, которое ведется в рамках трудовой деятельности и подразумевает общественный контроль со стороны работодателя. Также следует помнить, что сотрудник осуществляет трудовую деятельность в соответствии с Трудовым кодексом РФ, а значит, данный вид деятельности подлежит контролю государства. Отсюда следует, что мобильный мониторинг не касается частной жизни работника. Согласно ТК РФ, работник должен выполнять обязанности и соблюдать трудовую дисциплину, работодатель, в свою очередь, вправе требовать исполнения обязанностей сотрудником. А главное, обязан отслеживать фактически отработанное время, на что и нацелена система отслеживания мобильного телефона. Таким образом, она выступает как инструмент выполнения обязанностей руководителя согласно ТК РФ. Перемещения сотрудника в рабочее время также относятся к его трудовой деятельности, поэтому не являются предметом частной жизни и могут находиться под контролем работодателя.

Согласно законодательству, данные о трудовой деятельности человека являются персональными, в соответствии с ФЗ №152, в ряде случаев, предусмотренных данным

законом [3]. Один из них – это заключение договора, одной из сторон которого является работник, в конкретной ситуации это трудовой договор, по которому лицо несет определенные обязательства, необходимые для исполнения договора. В случае, чтобы оценить эффективность работы сотрудника, отслеживание мобильного телефона – это способ контроля исполнения сотрудником обязательств согласно заключенному договору.

Чтобы пользоваться таким методом контроля, следует поставить в известность сотрудника и отразить это в документах, но законодательно оформление используемых работодателем форм контроля не предусмотрено. Это обусловлено тем, что отслеживание мобильного телефона не подразумевает возложение на работника дополнительных обязанностей и не происходит изменений в трудовом договоре. Тем не менее, сотрудников лучше уведомить о такой системе контроля, так как это позволит ввести комплекс мер по мотивации персонала и повысить уровень ответственности по отношению к выполнению трудовых обязанностей.

Нужно понимать, что легальная слежка - это отслеживание местоположения пользователя, и только в том случае, если он дал на это разрешение.

Далее стоит рассмотреть ситуации, которые касаются частной жизни человека. Сбор информации о человеке без его согласия может быть незаконным, и слежка через смартфон тоже к этому относится. Однако, есть вполне легальные способы следить за чьим-то местоположением – специальные приложения для этих целей, которые может установить на смартфон любой желающий.

Легальная слежка возможна, если человек сам разрешил доступ к его личным данным. В частности, если он разрешил приложениям считывать информацию о его местоположении — GPS-трекинг его смартфона будет законным. Правда специальное ПО на этот смартфон еще надо будет установить.

Есть возможность следить за человеком со смартфоном, не устанавливая специального программного обеспечения. Например, если «объект» использует Карты Google, было бы удобно воспользоваться функцией «Показывать, где я» — всё, что нужно сделать, это включить его. Также для iOS есть встроенная функция «Найти iPhone», с её помощью можно определить геолокацию человека, только если активировать семейный доступ, то будет создана группа, которая внесётся в систему iPhone, и можно отслеживать всех членов группы. Android имеет подобную программу Find My Device.

Но если речь идёт о трекинге сотового телефона без согласия владельца, то очевидно, что отслеживать мобильный телефон законным способом можно лишь через оператора связи, для этого необходимо иметь постановление суда. Это сложный процесс, который занимает много времени. Операторы связи используют метод триангуляции для определения местонахождения устройства. Они подключают три ближайших вышки для того, чтобы засечь сигнал телефона и определить его местоположение, но данным методом зачастую могут пользоваться только органы власти.

Если говорить о нелегальных способах, то тут можно отметить Stingray или IMSI трекер, или симуляторы сотовой связи — это устройства, которые незаконно используются для отслеживания телефона. Stingray действует как вышка для мобильного телефона, заставляя устройства подключаться к нему. Современные смартфоны по-прежнему уязвимы для такого рода прослушивания. Мобильные телефоны считают, что они подключаются к сотовой вышке и перенаправляют все звонки и сообщения на трекер IMSI. При этом мобильный телефон должен находиться в пределах 2-х километров, чтобы можно было отследить его.

Нужно понимать, что незаконные действия преследуются по закону. Данные, которые находятся в смартфоне человека, считаются информацией из конфиденциальных источников. Доступ к ней возможен только с согласия владельца гаджета. Если решено собирать информацию об абоненте скрытно, нужно знать, что это нарушает Конституцию РФ, и на человека могут совершенно резонно подать в суд.

По 137 статье УК РФ «Нарушение неприкосновенности частной жизни», незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без согласия, грозит штрафом в размере от ста пятидесяти тысяч до трехсот пятидесяти тысяч рублей, лишением права занимать определенные должности или заниматься определенной деятельностью на срок от трех до пяти лет, либо тюремным сроком до пяти лет.

Установка шпионских программ подпадает под статью 272 «Неправомерный доступ к компьютерной информации». По ней можно получить штраф в размере до двухсот тысяч рублей, либо принудительные работы или лишение свободы на срок до двух лет.

Что касается областей применения трекинг-контроля, то можно выделить следующие:

- Контроль важных грузов;
- Контроль подчинённых/работников;
- Наблюдение за отдельно взятыми личностями (Розыск, поиск);
- Контроль над людьми, которые находятся под домашним арестом;
- Поиск мобильного устройства;
- Определение последней точки активности мобильного устройства;

Можно перечислить ещё множество областей применения, но следует отметить, что почти все пункты связаны с выполнением каких-либо специальных мероприятий, и зачастую будут выполняться представителями органов власти.

Список использованных источников

1. Алексей Голощапов Google Android. Создание приложений для смартфонов и планшетных ПК / Алексей Голощапов. - М.: "БХВ-Петербург", 2013. - 832 с.
2. Сильвен Ретабоуил Android NDK. Разработка приложений под Android на C/C++ / Сильвен Ретабоуил. - М.: "ДМК пресс. Электронные книги", 2014. - 496 с.

КОНФИГУРАЦИЯ СИСТЕМЫ MICROSOFT WINDOWS

Черных Анастасия Дмитриевна, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Конфигурация системы (она же MSConfig или сокращенно КС) — это среда, которая создана для управления автозагрузкой программ, параметрами запуска данного компьютера, а так же службами и так далее. Кратко говоря, это среда для настройки самых важных компонентов Windows.

Основное за что отвечает КС:

- режим запуска ОС
- автозагрузка приложений при старте работы
- работу служб
- запуск некоторых системных приложений
- удобную настройку служб для оптимизации ОС

Существует 3 способа, как и в случае с реестром:

- С помощью команды выполнить
- С помощью проводника
- С помощью поиска

В первом случае мы вводим в поиск команду выполнить затем в выведенную строку вводим MSConfig.

Следующий способ открытия КС - проводник. Открываем корневой диск С и идем по пути C:\Windows\System32. А затем запускаем файл msconfig.exe.

И самый элементарный способ - поиск. Нужно всего лишь открыть поиск и ввести все тот же msconfig.

КС состоит из 5 вкладок:

- Общие
- Загрузка
- Службы
- Автозагрузка
- Сервис

Дадим краткую характеристику каждой из вкладок.

Общие. В данной вкладке КС находятся варианты запуска системы. Чтобы лучше разбираться какой вариант запуска выбрать нужно рассмотреть из детальней, их всего 3.

Обычный запуск. Если выбрать данный вариант запуски, то вместе с компьютером запостятся все программы, стоящие на автозапуск, а также все приложения Windows. Рекомендуется после установки системы перейти с обычного режима на выборочный запуск. Тогда вместе с системой будут запускаться только выбранные программы.

При **диагностическом запуске** запускаются только основные приложения. Такой запуск может отключить, необходимые для возврата в обычный или выборочный режим, приложения.

При **выборочном запуске** запускаются только основные, а так же выбранные приложения.

Следующая вкладка - **загрузка**. В этой вкладке отображаются все находящиеся на компьютере установленные системы. В параметрах загрузки можно выбрать безопасный режим, тогда после перезагрузки он запустится в этом режиме.

Можно выбрать 4 варианта безопасного режима:

- Минимальная (система запустит необходимые службы, которые могут работать без подключения к интернету)
- Другая оболочка (открывается командная строка и запускается необходимые системные службы)

• Восстановление ActiveDirectory (запускается необходимые системные службы и службы ActiveDirectory)

• Сеть (запускаются необходимые системы и службы, а так же подключение к интернету; так же в этом варианте можно выбрать несколько пунктов

- Без GUI (отключает экран приветствия Windows)
- Журнал загрузки (сохраняет всю информацию о загрузке системы)
- Базовое видео (загружаются система с минимальным параметром VGA)
- Информация об операционной системе (при запуске все имена драйверов отображаются на экране)

Так же можно выбрать дополнительные параметры, такие как:

- Количество процессоров (показывает количество процессоров, которые должны использоваться при запуске системы)
- Максимум памяти (показывает максимальный объем физической памяти)
- Откладка (показывает глобальные параметры)
- Блокировка PCI (дает запрет на распределение ресурсов ввода)

Третья вкладка КС - **службы**. В этой вкладке отображаются все службы компьютера, а также состояние каждой службы (работает или остановлена).

Не все службы конфигурации можно отключить, так как без некоторых система просто не сможет работать. Чтобы точно знать какие службы можно отключить просто поставим галочку на нижнее окно «не отображать службы Майкрософт». Четвертая вкладка КС - **автозагрузка**. В этой вкладке отображаются все программы, которые запускались автоматически вместе с системой. Для удобства автозагрузка была перенесена в диспетчер задач во всех ОС после Windows 7. И последняя вкладка - **сервис**. В данной вкладке перечислены приложения, которые запускаются во время запуска системы.

НАРУШЕНИЕ ЦЕЛОСТНОСТИ ИНФОРМАЦИИ В КРИПТОГРАФИИ

Шарапа Екатерина Игоревна, 4 курс ФПСОИБ
Федеральное государственное казенное образовательное учреждение высшего образования
Московский университет МВД России имени В.Я. Кикотя, Москва

Прежде чем говорить о проблеме нарушении целостности в криптографии, стоит сказать о том, что такое криптография, что она из себя представляет и историю развития криптографии.

Итак, криптография- наука, изучающая обеспечение целостности данных, аутентификации (подлинности), конфиденциальности.

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифровывание и расшифровывание проводится с использованием одного и того же секретного ключа.

История криптографии насчитывает около 4 тысяч лет.

Вначале криптография заключалась в замене текста другим алфавитом или букв другими буквами, затем появились поли алфавитные шифры (используются до сих пор), а затем внедрением электромеханических устройств, после этого начался переход к математической криптографии. Современная криптография использует для своей работы как математику, так и информатики.

Также следует отметить, что такое нарушение целостности информации. Нарушение целостности информации - повреждение, приводящее к невозможности использовать информацию без восстановления. Помимо вероятности потерять важные данные, угрозе подвержена работоспособность всей.

По характеру нарушение целостности информации (данных) рассматривают:

- Саботаж – повреждение, наступившее в результате целенаправленных злонамеренных действий. В указанный пункт включаются атаки хакеров, деятельность сотрудников, решивших по разным причинам расстроить функционирование собственной компании. Встречаются и иные ситуации, обусловленные корыстными мотивами, местью и т.п. участников.

- Сбой программ. Связан с некорректной настройкой приложения, взломом или действиями вредоносных программ. Следует отметить, что по мере увеличения способов хранения, обработки, записи данных будет возрастать и количество рисков.

Методы обеспечения целостности информации

1. Отказоустойчивость — это способность компьютерной системы, электронной системы или сети обеспечивать бесперебойное обслуживание несмотря на то, что один или несколько его компонентов не работают. Отказоустойчивость также устраняет возможные прерывания обслуживания, связанные с программными или логическими ошибками. Цель состоит в том, чтобы предотвратить катастрофический сбой, который может возникнуть из-за единственной точки отказа.

Отказоустойчивость тесно связана с поддержанием непрерывности работы компьютерных систем и сетей. Отказоустойчивые среды определяются как те, которые мгновенно восстанавливают обслуживание после сбоя службы.

Отказоустойчивость связана со следующими техническими характеристиками систем:

· коэффициент готовности, который показывает, какую долю времени от общего времени службы система находится в рабочем состоянии;

· надёжность системы, которая определяется, например, как вероятность отказа в единицу времени.

2. Обеспечение безопасности восстановления.

Резервное копирование относится к копированию физических или виртуальных файлов, или баз данных на вторичный сервис для сохранения в случае отказа оборудования или другой катастрофы. Процесс резервного копирования данных имеет решающее значение для успешного плана аварийного восстановления

Предприятия резервируют данные, которые, по их мнению, уязвимы в случае ошибки программного обеспечения, повреждения данных, сбоя оборудования, вредоносного взлома, ошибки пользователя или других непредвиденных событий. Резервные копии захватывают и синхронизируют моментальный снимок момента времени, который затем используется для возврата данных в прежнее состояние.

Целостность информации в криптографии

При шифровании могут также возникать различные нарушения информации, таких как инверсия битов, удаление или добавление битов, изменение порядка следуемых битов.

Для проверки целостности информации в криптографии используется так называемая имитовставка (дополнительная информация). Эта информация вводиться к сообщению определенную комбинацию байт. Следуя определенным алгоритмом, можно выяснить была ли нарушена целостность информации третьей стороной.

Имитовставки деляться на два класса:

1. Коды, алгоритмы которых вычисляют целостность данной информации, путем хеширования информации (modification detection code).

2. Коды аутентификации. Это проверка подлинности данных хешированием с использованием секретного ключа.

Следует отметить, что такое хеширование.

Хеширование – это определенный алгоритм, способный преобразовывать массив данных в строку фиксированной длины. Одна и та же информация имеет одинаковый хэш, соответственно разная информация будет иметь разные хэши. Также хэш позволяет из достаточно большого объема получить маленький объем.

Можно привести пример использования хэширования для проверки целостности информации при передаче данных. Передав, например информацию, вы ее захэшировали. Получатель также захэшировал информацию этим же способом и отправил вам. Если хэши одинаковые, можно смело утверждать о целости информации при передаче.

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОСУЩЕСТВЛЕНИИ ДИСТАНЦИОННОЙ РАБОТЫ

Шарова Ксения Михайловна, 4 курс ФПСОИБ
Научный руководитель Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации им. В.Я. Кикотя», г. Москва

В связи с пандемией 2020 года, которая внесла коррективы не только в личную жизнь людей, но и в их работу, в частности перевод многих предприятий и организаций на удалённый формат. В связи с этим многим пришлось нелегко в плане перехода с обычного привычного вида деятельности вживую к дистанционному управлению и работе. Помимо сложностей с выполнением обязанностей, возложенных по договору, работники могли столкнуться и с проблемами, возникшими в результате деятельности злоумышленников, область действий которых распространяется на сеть Интернет и все, что с ней связано. Удаленный доступ: процесс получения доступа (через внешнюю сеть) к объектам доступа информационной системы из другой информационной системы (сети) или со средства вычислительной техники, не являющегося постоянно (непосредственно) соединенным физически или логически с информационной системой, к которой он получает доступ.

В целях принятия мер по противодействию коронавирусной инфекции предусмотрен перевод работников на дистанционный режим исполнения должностных обязанностей, обеспечивающий бесперебойное функционирование федеральных органов исполнительной власти и подведомственных организаций Для качественного и безопасного удаленного доступа можно определить некоторые правила, соблюдение которых окажет положительное влияние на безопасность информационных систем, используемых работниками на «дистанционке».

Во-первых, для сотрудников, подключающихся к сети предприятия из дома, должна быть осуществлена многофакторная аутентификация, то есть проверка подлинности лица, подключающегося к данной сети, должна быть утверждена самим лицом и проверена.

Во-вторых, при попытках удаленного доступа, возможно, злоумышленником, данные сведения должны регистрироваться в журналах и проверяться.

В-третьих, должен осуществляться мониторинг и контроль удаленного доступа, иначе данные, хранимые на серверах компании могут попасть в руки конкурентам и нанести огромный ущерб предприятию.

В-четвертых, технические специалисты и специалисты по информационной безопасности должны обеспечить доверенный канал связи при удаленном доступе к системе. И в-пятых, должны быть установлены и задокументированы виды доступа, которые разрешены при удаленном доступа к системе.

В случае невозможности применения специально предназначенных для удаленного доступа средств вычислительной техники допускается применение личных средств вычислительной техники при условии реализации технологии загрузки и работы по удаленному доступу к информационной системе государственного органа (организации) с защищенного съемного машинного носителя информации по технологии LiveUSB.

При использовании личных средств вычислительной техники для обеспечения дистанционной работы могут возникнуть дополнительные угрозы, такие как: перехват информации по каналам передачи данных, передаваемых между LiveUSB и информационной системой; запуск LiveUSB с неавторизованного СВТ; утечка защищаемой информации за счет подключения сторонних периферийных устройств к личному СВТ при работе на LiveUSB; несанкционированное копирование защищаемой информации с Live USB на носители личного СВТ и т.д. Применив следующие меры защиты можно избежать данных проблем: сертифицирование средства доверенной загрузки, применение сертифицированной

операционной системы, применение двухфакторной аутентификации, дистанционный доступ к системе через технологию RDP, VDI, централизованной управление Live USB и удаленное администрирование.

Это далеко неисчерпывающий список, применяемых для информационной безопасности мер при удаленной работе, однако основные были затронуты. Каждый руководитель должен сам решать в какой мере ему стоит защитить своё предприятие от нежелательной утечки и принять меры, главное, чтобы это все было вовремя.

ГОСУДАРСТВЕННАЯ СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РАЗРАБОТКА РОССИЙСКОГО ПО

Шитов П.М., Чапля Д.Я., курсанты 992 взвода
Научный руководитель Овчинский Анатолий Семенович, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий, доктор технических наук, профессор
Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя», г. Москва

1. Государственные системы защиты информации

Представляют собой совокупность органов и исполнителей, используемой ими техники и структуры защиты информационных данных и технологий, а также защищаемые объекты, организованные и функционируемые по правилам, установленным соответствующим правовым, организационно-распорядительным и нормативным документам в области защиты информации и информационных технологий. Так же являются составной частью системы обеспечения национальной безопасности РФ и призвана защитить безопасность государственных органов, а также граждан и жителей страны от внутренних и внешних угроз в сфере информационной безопасности и деятельности.

ФСТЭК РФ-это главный государственный орган, осуществляющий деятельность по защите технической защиты информации на федеральном, межрегиональным, региональном, отраслевом и объектовом уровнях.

Государственный орган включает в себя множество служб и структур, которые так же являются подсистемами лицензирования деятельности предприятий в области информационной безопасности, сертификации средств защиты информации и сертификации объектов информатизации в соответствии с требованиями информационной безопасности.
Вышеперечисленные подсистемы представляют в совокупности деятельность следующих органов:

Федеральная служба технического и экспортного контроля (ФСТЭК России) и ее территориальные органы (региональные управления в субъектах Российской Федерации)
Федеральные органы исполнительной власти, другие органы и организации Российской Федерации, руководящие работники которых входят в состав коллегии ФСТЭК России по должности (Минюст, Минобороны, МЧС, МВД, МИД, Минпромэнерго, Минэкономразвития, Минприроды, ФСО, ФСБ, СВР, ГУСП, РАН, ЦБР)

Структурные подразделения по защите информации федеральных органов исполнительной власти, других органов государственной власти и организаций Российской Федерации.

- Предприятия, проводящие работы с использованием сведений, отнесенных к информации ограниченного доступа, и их подразделения по защите информации
- Научно-исследовательские организации по проблемам защиты информации
- Организации-разработчики средств защиты информации, защищенных технических средств и средств контроля эффективности защиты информации.
- Предприятия, оказывающие услуги в области защиты информации.
- Организации Федерального агентства по техническому регулированию и метрологии (бывшего Госстандарта России), выполняющие работы по стандартизации в области защиты информации.
- Органы системы лицензирования деятельности в области защиты информации.

Функционирование государственной системы защиты информации осуществляется на основании законности:
Конституция Российской Федерации

- ФЗ «О безопасности»

- ФЗ «О государственной тайне»
- ФЗ «Об информации, информатизации и защите информации»
- ФЗ «Об участии в международном информационном обмене»
- Доктрина информационной безопасности Российской Федерации
- Положение о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от утечки по техническим (утверждено Постановлением Совета Министров – Правительства Российской Федерации от 15 сентября 1993 г. №912–51)
- Указы президента Российской Федерации (№1085 от 16.8.2004 г.)
- Постановления правительства Российской Федерации

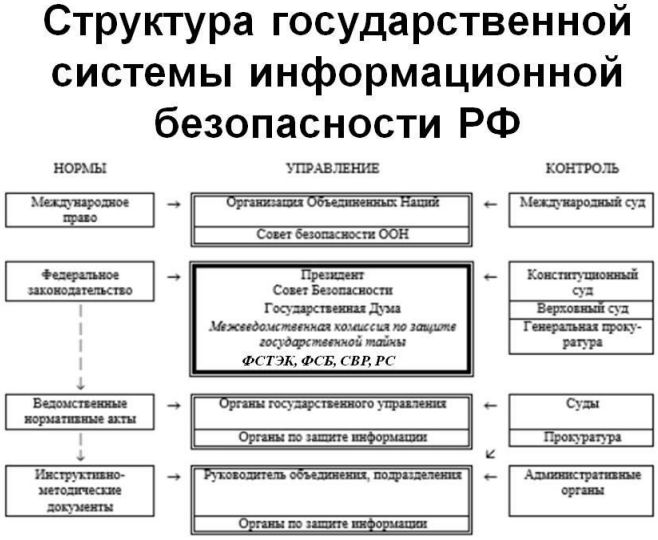


Рисунок 1 – структура государственной системы безопасности РФ

2. Российское программное обеспечение

Отечественными (российскими) производителями программного обеспечения (ПО), занимающимися производством собственного (проприетарного) ПО или «свободного программного обеспечения» (СПО), либо предоставляющих услуги по разработке, тестированию и поддержке ПО по заказам сторонних организаций, могут быть признаны российские юридические лица, в которых не менее чем 51% долей в уставном капитале или акций, производных инструментов и других инструментов корпоративного контроля принадлежат прямо или косвенно российским гражданам или государственным образованиям, а также физическим лицам, являющимся гражданами и налоговыми резидентами РФ.

Последовательность событий:

2021: Минцифры намерено запретить иностранный софт в школах РФ

2020: ИТ-компании предложили Минцифры устанавливать отечественную ОС на все компьютеры

2016: Выделение 5 млрд рублей на финансирование разработки ПО

2015: Утверждены правила формирования реестра отечественного ПО

2014: Мнкомсвязи ищет деньги на финансирование разработки отечественного ПО

30 июля 2014: Обсуждения определения "Отечественного ПО" в Думе

О необходимости форсированного развития отечественного рынка ПО, обеспечения максимальной независимости от иностранных разработок в сфере высоких технологий и сохранения информационного суверенитета впервые на высшем уровне заговорили в 2014 году, когда санкции США и Евросоюза резко повысили риски, связанные с применением зарубежного софта в бизнесе и государственных организациях. Именно тогда в Министерстве связи и массовых коммуникаций РФ всерьёз озадачились решением этого

стратегически значимого, по мнению чиновников, вопроса вместе со стимулированием спроса на национальные продукты и проработкой соответствующих мер поддержки отечественных разработчиков. Как результат — в кратчайшие сроки на законодательном уровне были утверждены ограничения на допуск иностранного ПО при осуществлении государственных и муниципальных закупок, а также правила формирования и ведения единого реестра российских программ. Всё это положительным образом отразилось на рынке программного обеспечения в России, который за последнее время пополнился множеством интересных проектов и разработок. В том числе и в области операционных систем.

«Альт Линукс СПТ» представляет собой унифицированный дистрибутив на базе Linux для серверов, рабочих станций и тонких клиентов со встроенными программными средствами защиты информации, который может быть использован для построения автоматизированных систем по класс 1В включительно и информационных систем персональных данных (ИСПДн) по класс 1К включительно.

Платформа «Альт» — это набор Linux-дистрибутивов уровня предприятия, позволяющих развернуть корпоративную IT-инфраструктуру любого масштаба. В состав платформы входят три дистрибутива. Это универсальный «Альт Рабочая станция», включающий в себя операционную систему и набор приложений для полноценной работы
Российский проект по созданию экосистемы программных продуктов на базе дистрибутива Linux, предназначенных для комплексной автоматизации рабочих мест и IT-инфраструктуры организаций и предприятий, в том числе в дата-центрах, на серверах и клиентских рабочих станциях. Платформа представлена в вариантах «ОСь.Офисная» и «ОСь.Серверная». Они различаются наборами включённого в дистрибутив прикладного ПО.

Разработка научно-производственного объединения «РусБИТех», представленная в двух вариантах: Astra Linux Common Edition (общего назначения) и Astra Linux Special Edition (специального назначения). Семейство операционных систем ROSA Linux включает внушительный набор решений, предназначенных для домашнего использования (версия ROSA Fresh) и применения в корпоративной среде (ROSA Enterprise Desktop), развёртывания инфраструктурных IT-служб организации (ROSA Enterprise Linux Server), обработки конфиденциальной информации и персональных данных (РОСА «Кобальт»), а также составляющих государственную тайну сведений (РОСА «Хром» и «Никель»).

Мобильная система Вооружённых Сил (МСВС) Разработчик: Всероссийский научно-исследовательский институт автоматизации управления в непромышленной сфере им. В. В. Соломатина (ВНИИНС). Защищённая операционная система общего назначения, предназначенная для построения стационарных и мобильных защищённых автоматизированных систем в Вооружённых Силах Российской Федерации. Принята на снабжение в ВС РФ в 2002 году. В основу МСВС положены ядро и компоненты Linux, дополненные дискреционной, мандатной и ролевой моделями разграничения доступа к информации.
Далее предлагаю рассмотреть структуру ИТ в Российской Федерации:

Рисунок 2 – Структура ИТ в Российской Федерации

СОВРЕМЕННЫЙ УРОК ЛИТЕРАТУРЫ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

Шопинский Андрей Олегович, студент 4-го курса
Научный руководитель Цыгуль Оксана Владимировна, преподаватель
Старооскольский технологический институт им. А.А. Угарова (филиал) федерального государственного автономного образовательного учреждения высшего образования «Национальный исследовательский технологический университет «МИСиС»
Оскольский политехнический колледж, г. Старый Оскол

В настоящее время существует ряд причин, приводящих к тому, что ученики всё реже берут в руки книги. Главная из них заключается в том, что современные школьники рождены в эпоху цифровых технологий. По мнению учёных, самое заметное влияние эти технологии оказали на повседневную жизнь людей, благодаря чему возникло новое информационное общество,кардинально отличающееся от общества традиционного.

Цель работы – проанализировать основные методы работы с литературным материалом при помощи компьютерных технологий. В соответствии с целью были определены следующие задачи:

1. Определить ряд проблем современной методики преподавания классической литературы школьникам;
2. Представить актуальные способы преподавания литературы;
3. Продемонстрировать одну из эффективных цифровых технологий работы с текстом.

В обществе, сложившемся под воздействием технического прогресса, учёные выделяют "цифровых иммигрантов", людей, не так хорошо знакомых с цифровыми технологиями, и "детей цифровой эры", то есть тех, кто большую часть своей жизни проводит в сети Интернет и не делает различия между жизнью в Сети и жизнью вне неё. Такое деление приводит к трудностям в педагогическом общении. Учителя являются "цифровыми иммигрантами", которые привыкли к традиционному способу восприятия информации, им приходится сегодня осваивать новые технологии, прилагая большие усилия, в то время как для "детей цифровой эры" современная информационная среда интуитивно понятна, привычна и комфортна.

Чем отличаются представители цифрового поколения от вчерашних выпускников школ? По мнению учёных, дети цифрового поколения:

- большую часть своей жизни проводят в Сети;
- умеют выполнять несколько задач одновременно;
- склонны использовать цифровые технологии для получения информации.

Знание этих особенностей может помочь учителю мотивировать учащихся к чтению при помощи тех средств и технологий, которые более привлекательны для подростков. Обратившись к опыту конкретных педагогов, приведём примеры технологических и методических приёмов, использование которых может способствовать появлению интереса к чтению у учащихся. Задача педагога – учесть потребности школьного возраста и подать материал таким образом, чтобы у учеников появился интерес к изучению определённой темы и к чтению художественного произведения в целом. Следует выделить ряд современных методов преподавания художественной литературы обучающимся.

1. Создание проблемных ситуаций посредством визуальных образов.

Например, можно показать ребятам слайд со странным колодцем и спросить, что тут изображено. После того как высказаны различные гипотезы, учитель говорит о том, что на фотографии запечатлён... памятник сожжённым книгам в Берлине. После этого организует беседу о том, что книги в разные времена и в разных странах уничтожались, запрещались, истреблялись. Далее идёт обсуждение и каждый делает свои выводы.

2. Использование видеороликов при введении нового материала.

Оснащение школьных кабинетов сегодня даёт возможность учителю использовать на уроке видеоролики. Небольшой фрагмент художественного или учебного фильма может привлечь учеников к чтению, если он умело введён в структуру урока. Вариантов использования видео много.

Один из них: учитель может продемонстрировать кульминационный момент из экранизации художественного произведения, изучаемого в классе, но не показывать развязки. О том, что происходило дальше, чем разрешилась ситуация, ученикам предстоит узнать из книги.

Всё большую популярность среди учеников, учителей и библиотекарей приобретает ещё одна разновидность видеороликов – "буктрейлер". Буктрейлер – это ролик-миниатюра, который включает в себя самые яркие и узнаваемые моменты книги, визуализирует её содержание. Представляя читателю книги и пропагандируя книгочтение в мировом культурном сообществе, буктрейлеры превратились в отдельный самобытный жанр, объединяющий литературу, визуальное искусство и Интернет.

3. Введение нового материала при помощи интерактивных экскурсий.

Виртуальные экскурсии – экскурсии, которые позволяют при помощи мультимедийных ресурсов совершить путешествие по местам жизни и творчества писателей, погрузиться в мир произведений автора на уроках литературы. Эффективным приемом здесь также может быть знакомство с историей памятников великим писателям или скульптурными композициями, созданными по мотивам русской классики, с обязательным анализом художественной идеи и значимости этого произведения искусства.

4. Создание сайтов, блогов для демонстрации творческих проектов по литературе.

Работа с "облачными" сервисами открывает множество возможностей для педагога и учеников и заслуживает отдельного внимания. Вот один из примеров такой работы. Во время изучения творчества А.С. Пушкина обучающиеся класса получили задание выбрать любое понравившееся стихотворение поэта и сделать к нему слайд-шоу при помощи удобных для них программ. После окончания работы над проектом перед ними стояли задачи: разместить получившуюся работу на youtube и оформить собственную страницу на сайте "Творческие проекты по литературе", созданном педагогом. Работа над небольшим проектом позволила учителю не только привлечь к осмысленному чтению стихотворений А.С. Пушкина, но и сформировать у обучающихся ИКТ-компетенции.

5. Привлечение учеников к участию в литературных конкурсах и викторинах в сети Интернет. Такой вид деятельности формирует опыт публичного выступления, позволяет оценить со стороны свой уровень речевой культуры.

6. Привлечение обучающихся к чтению литературных журналов в сети Интернет. Это позволит расширить представление о современных тенденциях в литературе. Проявить себя в литературном творчестве.

Современный мир IT-технологий достаточно разнообразен, и на сегодняшний день можно найти много веб-сервисов и программных продуктов, позволяющих сократить время или упростить жизнь людям разных профессий. Остановимся на веб-приложении, разработанном студентами в рамках курсового проекта в Оскольском Политехническом Колледже СТИ НИТУ МИСиС. Приложение «SPEAKER» – система перевода голосового сообщения в текстовый формат.

С использованием данного приложения можно производить конвертацию голоса в текст в режиме реального времени, а также сохранять введённый текст в базе данных для дальнейшего использования. Система способна синтезировать речь, то есть сразу после перевода можно прослушать свой текст и исправить ошибки. Такое приложение может

использовать журналист для быстрой записи своих мыслей или описания происходящих вокруг событий. Данная программа может быть полезна авторам для редактирования художественного текста, а также начинающим ораторам, чтобы добиться чистоты и правильности речи, повысить уровень коммуникативной культуры.

Таким образом, современные цифровые технологии повышают эффективность работы с художественным текстом у подростков, формируя одновременно эстетические и технические компетенции в соответствии с интересами и потребностями молодого читателя. Представленная технология приложения "SPEAKER" – пример актуального использования компьютерных технологий в гуманитарной сфере.

Список использованных источников

1. Квашина Е. С. Литература и компьютер: в ожидании перезагрузки. Журнал для учителей словесности "Литература", 2015. - № 2. – С. 57-59.

2. Фефилова Г. Е. Литература. 11 класс. Планы-конспекты для 105 уроков. – М., 2016. – 447 с.

3. Онлайн-учебник по языку программирования JavaScript - https://learn.javascript.ru

КОНЦЕПЦИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Шульга Даниил Станиславович, курсант 3-го курса
Казанцев Владимир Иванович, преподаватель кафедры СИТ УНК ИТ
Федеральное государственное казенное образовательное учреждение высшего образования Московский университет МВД России имени В.Я. Кикотя, Москва

Концепция обеспечения информационной безопасности органов внутренних дел Российской Федерации до 2020 года[1] определяет комплекс мер, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем органов внутренних дел Российской Федерации[2] от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам.

Правовую основу Концепции составляют Стратегия национальной безопасности Российской Федерации до 2020 года[3], Доктрина информационной безопасности Российской Федерации[4], Стратегия развития информационного общества в Российской Федерации[5], а также нормы законодательства Российской Федерации и нормативные правовые акты Министерства внутренних дел Российской Федерации[6], регулирующие вопросы обеспечения информационной безопасности.

Концепция определяет цели, задачи, принципы и основные направления обеспечения информационной безопасности ОВД.

Положения Концепции учитываются при разработке программ, реализации мероприятий и инициатив, связанных с обеспечением информационной безопасности ОВД, на период до 2020 года включительно.

Концепция реализуется на федеральном, окружном, межрегиональном, региональном и районном уровнях управления МВД России.

В настоящей Концепции используются следующие основные понятия:

информационная безопасность ОВД – состояние защищенности информации, информационных ресурсов и информационных систем ОВД, при котором обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования;
«облачная архитектура» – технология распределенной обработки данных, предоставляющая конечному пользователю вычислительные мощности в виде интранет-сервиса;
система обеспечения информационной безопасности ОВД – совокупность правовых, организационных и технических мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам информационной безопасности с целью предотвращения или существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней;
технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды передачи информации и средств, с помощью которых добывается защищаемая информация;
угроза информационной безопасности ОВД – совокупность условий и факторов, создающих потенциальную или реальную опасность утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней.

Состояние информационной безопасности ОВД

В органах внутренних дел Российской Федерации на постоянной основе проводится работа по защите информации, информационных ресурсов и информационных систем ОВД.

В целях создания эффективной системы обеспечения информационной безопасности осуществляется комплекс мероприятий по защите информации, содержащей сведения, составляющие государственную тайну, и сведения конфиденциального характера, по

противодействию техническим разведкам противника, предотвращению утечки информации по техническим каналам, несанкционированного доступа к ней.

Организована работа по лицензированию и аккредитации ОВД в качестве органов по аттестации объектов информатизации по требованиям безопасности информации[1], оснащению их современными средствами защиты информации, контрольно-измерительной и поисковой техникой.

Оснащение подразделений МВД России средствами защиты информации осуществляется в рамках государственного оборонного заказа в пределах выделяемого МВД России финансирования.

По состоянию на январь 2012 года 52 подразделения МВД России имеют аттестат аккредитации и оснащены необходимым комплектом контрольно-измерительной и поисковой техники, что позволяет им проводить аттестацию объектов информатизации по требованиям безопасности информации.

Проводится работа по подготовке специалистов в области технической защиты информации на базе федеральных государственных казенных образовательных учреждений высшего профессионального образования «Академия управления МВД России» и «Воронежский юридический институт МВД России».

Вместе с тем в настоящее время не в полной мере решены следующие вопросы: приведение ведомственной нормативной правовой базы в соответствие с законодательством Российской Федерации, регулирующим вопросы обеспечения защиты информации; обеспечение ОВД требуемым объемом средств защиты информации, в том числе криптографическими средствами, необходимыми для организации технической защиты информации;

создание сети органов по аттестации объектов информатизации и оснащению их современными средствами защиты информации, контрольно-измерительной и поисковой техникой;

организация профессиональной подготовки и переподготовки сотрудников подразделений МВД России в области информационной безопасности.

Цели, задачи и принципы обеспечения информационной безопасности ОВД

Целью обеспечения информационной безопасности ОВД является достижение с использованием методов технической, в том числе криптографической, защиты информации необходимого уровня защиты от специальных программно-технических воздействий, средств технических разведок, несанкционированного доступа, а также утечки информации по техническим каналам.

Основными задачами обеспечения информационной безопасности ОВД являются: совершенствование правовых, научно-практических, нормативно-технических, организационно-методических и иных основ информационной безопасности ОВД; реализация комплекса организационных (режимных) и технических мероприятий, направленных на обеспечение защиты информации, информационных ресурсов и информационных систем ОВД от утечки, хищения, утраты, несанкционированного доступа, уничтожения, искажения, модификации, подделки, копирования, блокирования; создание и развитие системы информационной безопасности ОВД с учетом реализации «облачной архитектуры»;

формирование и совершенствование системы мониторинга состояния информационной безопасности ОВД;

организация и совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности.

Информационная безопасность ОВД должна реализовываться на основе принципов законности, достаточности, оперативности, системности, комплексности, целенаправленности, приоритетного использования отечественных средств и систем защиты информации.

Основные направления обеспечения информационной безопасности ОВД

Решение поставленных задач осуществляется в ходе реализации следующих основных направлений:

выработка основных направлений единой научно-технической политики в области обеспечения информационной безопасности ОВД;

совершенствование нормативной правовой базы по обеспечению информационной безопасности ОВД;

развитие сети органов по аттестации объектов информатизации на базе подразделений информационных технологий, связи и защиты информации и оснащение их современными средствами защиты, контрольно-измерительной и поисковой техникой;

разработка новых и совершенствование существующих способов, методов и средств выявления, оценки, прогнозирования, нейтрализации и ликвидации угроз информационной безопасности ОВД;

организация технической защиты информации, программных, программно-технических и технических средств защиты, в том числе криптографической;

реализация разрешительной системы доступа к информационным ресурсам и информационным системам ОВД;

обеспечение информационной безопасности при межведомственном информационном взаимодействии с федеральными органами государственной власти;

разработка и совершенствование защищенных информационных технологий и информационно-телекоммуникационных систем ОВД;

организация защиты информации в единой информационной системе централизованной обработки данных[1] от несанкционированного доступа к обрабатываемой информации и воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;

обеспечение защищенного доступа пользователей к информационным ресурсам ЕИС ЦОД;

осуществление контроля целостности системы обеспечения информационной безопасности ОВД;

проведение оценки уязвимости и рисков информации при имеющемся множестве угроз и каналов утечки;

проведение технического аудита состояния защищенности информационных систем ОВД;

совершенствование профессиональной подготовки и переподготовки сотрудников органов внутренних дел в области обеспечения информационной безопасности на базе образовательных учреждений системы МВД России;

совершенствование материально-технической базы ведомственных образовательных учреждений.

Список использованных источников

Нормативно-правовые документы

1. Указ Президента РФ от 21.12.2016 N 699 (ред. от 25.12.2019) "Об утверждении Положения о Министерстве внутренних дел Российской Федерации и Типового положения о территориальном органе Министерства внутренних дел Российской Федерации по субъекту Российской Федерации";
2. Приказ МВД России от 31 декабря 2019 г. N 995 "Об утверждении Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом (загранаппарате Министерства внутренних дел Российской Федерации)"
3. Федеральный закон "О полиции" от 07.02.2011 N 3-ФЗ

4. Указ Президента РФ от 01.03.2011 N 248 (ред. от 13.07.2020) "Вопросы Министерства внутренних дел Российской Федерации" (вместе с "Положением о Министерстве внутренних дел Российской Федерации")
5. Указ Президента РФ от 11.07.2004 N 865 (ред. от 17.09.2020) "Вопросы Министерства иностранных дел Российской Федерации"
6. Доктрина информационной безопасности Российской Федерации. (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. № 646)
7. Глава 2 Положения о представительствах и представителях Министерства внутренних дел Российской Федерации за рубежом: приложение к приказу МВД России от 31.12.2019 № 995

Электронные ресурсы

1. https://elibrary.ru/
2. https://xn--b1aew.xn--p1ai/
3. https://www.mid.ru/ru/home
4. https://books.google.ru/

СОДЕРЖАНИЕ

Направление 1
Возможности современной студенческой проектной, исследовательской и научной деятельности и ее практическая реализация
СЕКЦИЯ 1.1

СЕКЦИЯ 1.2

СЕКЦИЯ 1.3

СЕКЦИЯ 1.6

СЕКЦИЯ 2.2

Материалы Всероссийской научно-исследовательской конференции с международным участием «Ломоносовские чтения – 2021» преподавателей и обучающихся образовательных организаций общего, среднего профессионального и высшего образования Российской Федерации.

Издано в авторской редакции.

Компьютерная верстка, дизайн:
Метлина Н.С.
Технический редактор:
Чедия А.А.

Электронный ресурс удаленного доступа:
http://sf-misis.ru/
Старый Оскол, микрорайон Макаренко, 42