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»
СТИ НИТУ «МИСИС»

Рабочая программа утверждена
решением Ученого совета
СТИ НИТУ «МИСИС»
от «20» июня 2023 г.
протокол № 5

Рабочая программа дисциплины

Защита информации

Закреплена за кафедрой **Кафедра автоматизированных и информационных систем управления**

Направление подготовки 13.03.02 Электроэнергетика и электротехника

Профиль Электропривод и автоматика

Квалификация **Бакалавр**

Форма обучения **Очная**

Общая трудоемкость **5 ЗЕТ**

Часов по учебному плану 180

в том числе:

аудиторные занятия 34

самостоятельная работа 110

часов на контроль 36

Формы контроля в семестрах: экзамен 3

Распределение часов дисциплины по семестрам

Семестр	3		Итого	
Вид занятий	УП	РП	УП	РП
Лекции	17	17	17	17
Практические	17	17	17	17
Контактная работа	34	34	34	34
Сам. работа	110	110	110	110
Часы на контроль	36	36	36	36
Итого:	180	180	180	180

Год набора 2023 г.

Программу составили:

доцент каф. АИСУ,
кандидат технических наук
Козырь Ольга Феликсовна
Должность,уч.ст., уч.зв ФИО полностью *подпись*

доцент каф. АИСУ,
кандидат технических наук
Соловьев Антон Юрьевич
Должность,уч.ст., уч.зв ФИО полностью *подпись*

Рабочая программа дисциплины
Защита информации
наименование

Разработана в соответствии с ОС ВО НИТУ МИСИС:
Самостоятельно устанавливаемый образовательный стандарт высшего образования - бакалавриат Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСИС» по направлению подготовки 13.03.02 Электроэнергетика и электротехника (приказ от 05.03.2020 г. № 95 о.в.)

Составлена на основании учебного плана 2023 года набора:
13.03.02 Электроэнергетика и электротехника,
Профиль: Электропривод и автоматика, утвержденного Ученым советом СТИ НИТУ «МИСИС»
«20» июня 2023 г., протокол № 5

Рабочая программа одобрена на заседании кафедры
Автоматизированных и информационных систем управления
наименование кафедры

Протокол от«24» мая 2023 г. № 03

и.о. зав. кафедрой АИСУ Д.А. Полещенко
аббревиатура наименования кафедры *подпись* *И.О. Фамилия*

«24» мая 2023 г.

Руководитель ОПОП ВО
и.о. зав. кафедрой АИСУ, кандидат
технических наук, доцент Д.А. Полещенко
должность, уч.ст., уч.зв. *подпись* *И.О. Фамилия*

«24» мая 2023 г.

1. ЦЕЛИ ОСВОЕНИЯ
Цель дисциплины – формирование теоретических знаний в области управления информационными ресурсами систем и сетей и отработка умений и навыков использования инструментальных программных систем, сетевых служб и оборудования для защиты информации в компьютерных системах. Задачи дисциплины: • Научить обучающихся основным терминам и понятиям защиты информации; • Научить обучающихся применять теоретические знания в области защиты информации для решения конкретных практических задач по выбранному направлению подготовки; • Научить обучающихся основным угрозам защиты информации и способам их предотвращения; • Научить обучающихся разбираться в типовых атаках направленных на ИС и программные продукты; Научить обучающихся основным видам криптографических алгоритмов и их уязвимостей

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Математика
2.1.2	Информатика
2.1.3	Правовые основы профессиональной деятельности
2.2	**Дисциплины и практики, для которых освоение данной дисциплины необходимо как предшествующее:**
2.2.1	Вычислительные средства и системы
2.2.2	Технические средства автоматизации

3. ИНДИКАТОРЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ, СОВМЕЩЕННЫЕ С РЕЗУЛЬТАТАМИ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ	
УК-1: Способен осуществлять поиск, критический анализ и синтез информации, умение анализировать процессы и системы с использованием соответствующих аналитических, вычислительных и экспериментальных методов, применять системный подход для решения поставленных задач	
Знать:	УК-1-З1 Знать основные понятия и термины, связанные с информационной безопасностью; УК-1-З2 Знать основные виды угроз информационной безопасности; УК-1-З3 Знать механизмы аутентификации и идентификации при доступе к информационным ресурсам; УК-1-З4 Знать основные криптографические алгоритмы; УК-1-З5 Знать нормативную и законодательную базу в области информационной безопасности
ОПК-3: Способен осуществлять моделирование, анализ и эксперименты в целях проведения детального исследования для решения задач в профессиональной области, использовать методы анализа и моделирования электрических цепей и электрических машин	
Уметь:	ОПК-3-У1 Уметь реализовывать различные криптографические алгоритмы ОПК-3-У2 Уметь реализовывать различные хэш-функции и электронно-цифровые подписи
Владеть:	ОПК-3-В1 Владеть навыками проведения анализа устойчивости различных криптографических алгоритмов

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр	Часов	Компетен-ции	Литература и эл. ресурсы	Примечание
	Раздел 1. Основные понятия и определения. Виды угроз					
1.1	Основные понятия и определения. Виды угроз /Лек/	3	2	УК-1-З1 УК-1-З2	Л 1.2 Л 1.3 Л 2.2 Л 3.1 Э 2 Э 3	Тест
1.2	Проработка лекционного материала. Самостоятельное изучение литературы. /Ср/	3	4	УК-1-З1 УК-1-З2	Л 1.2 Л 1.3 Л 2.2 Л 3.1 Э 2 Э 3	Тест

	Раздел 2. Социальная инженерия					
2.1	Социальная инженерия /Лек/	3	2	УК-1-З1 УК-1-З2	Л 3.1 Э 2 Э 3	Тест
2.2	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. /Ср/	3	4	УК-1-З1 УК-1-З2	Л 3.1 Э 2 Э 3	Тест
	Раздел 3. Понятия криптографии. Симметричные криптосистемы					
3.1	Понятия криптографии. Симметричные криптосистемы /Лек/	3	2	УК-1-З4	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Э 3	Тест
3.2	Шифрование данных методом замены в симметричных криптосистемах /Пр/	3	2	ОПК-3-У1	Л 3.2 Э 3	Тест
3.3	Шифрование с использованием метода гаммирования и датчиков псевдослучайных чисел. Одноразовые блокноты /Пр/	3	2	ОПК-3-У1	Л 3.2 Э 3	Тест
3.4	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. Выполнение домашних заданий. /Ср/	3	20	ОПК-3-У1 УК-1-З4 ОПК-3-В1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Л 3.2 Л 3.3 Э 3	Тест
	Раздел 4. Асимметричные криптосистемы					
4.1	Асимметричные криптосистемы /Лек/	3	2	УК-1-З4	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Э 1 Э 2 Э 3	Тест
4.2	Шифрование данных в асимметричной криптосистеме RSA/Пр/	3	3	УК-1-З4 ОПК-3-У1	Л 3.2 Э 3	Тест
4.3.	Алгоритм Диффи-Хелмана для безопасного обмена ключами /Пр/	3	3	УК-1-З4 ОПК-3-У1	Л 3.2 Э 3	Тест

4.4	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. /Ср/	3	10	УК-1-З4	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Л 3.2 Э 1 Э 2 Э 3 Э 3	Тест
	Раздел 5. Электронная цифровая подпись и хэш-функции. Криптоанализ					
5.1	Электронная цифровая подпись и хэш-функции. Криптоанализ /Лек/	3	3	УК-1-З4 УК-1-З3	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Э 1 Э 2 Э 3	Тест
5.2	Алгоритм электронной цифровой подписи RSA /Пр/	3	3	УК-1-З4 ОПК-3-У2	Л 3.2 Э 3	Тест
5.3	Алгоритм электронной цифровой подписи Эль-Гамаля /Пр/	3	4	УК-1-З4 ОПК-3-У2	Л 3.2 Э 3	Тест
5.4	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическому занятию. Выполнение домашнего задания /Ср/	3	20	УК-1-З4 ОПК-3-В1 ОПК-3-У2	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Л 3.2 Л 3.3 Э 1 Э 2 Э 3	Тест
	Раздел 6. Блокчейн и криптовалюта)					
6.1	Блокчейн и криптовалюта /Лек/	3	2	УК-1-З4 УК-1-З3	Л 3.1 Э 2 Э 3	Тест
6.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	3	6	УК-1-З4 УК-1-З3	Л 3.1 Э 2 Э 3	Тест
	Раздел 7. Идентификация и аутентификация	3				
7.1	Идентификация и аутентификация/Лек/	3	2	УК-1-З3	Л 1.1 Л 3.1 Э 1 Э 3	Тест
7.2	Проработка лекционного материала. Самостоятельное изучение литературы	3	6	УК-1-З3	Л 1.1 Л 3.1 Э 1 Э 3	Тест

	/Ср/					
	Раздел 8. Правовое регулирование информационной безопасности в РФ					
8.1	Правовое регулирование /Лек/	3	2	УК-1-З5	Л 1.1 Л 1.2 Л 1.3 Л 3.1 Э 1 Э 2 Э 3	Тест
8.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	3	4	УК-1-З5	Л 1.1 Л 1.2 Л 1.3 Л 3.1 Э 1 Э 2 Э 3	Тест
	Часы на контроль /Контроль/	3	36	УК-1-З1 УК-1-З2 УК-1-З3 УК-1-З4 УК-1-З5 ОПК-3-У1 ОПК-3-У2 ОПК-3-В1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.1 Л 3.2 Л 3.3	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Вопросы для самостоятельной подготовки к экзамену (зачёту с оценкой)

Раздел 1. Основные понятия и определения. Виды угроз

1. Понятие защиты информации. Комплекс мер безопасности. (*УК-1-31)*
2. Техногенные, антропогенные и стихийные источники угроз защиты информации (*УК-1-32)*
3. Внешние и внутренние угрозы. Умышленные и неумышленные угрозы (*УК-1-32)*
4. Классификация угроз безопасности по способам воздействия на объекты информационной безопасности угрозы (*УК-1-32)*

Раздел 2. Социальная инженерия

1. Определение социальной инженерии. Схема социальной инженерии (*УК-1-31)*
2. Претекстинг. Фишинг. Плечевой серфинг (*УК-1-32)*
3. Смишинг. Вишинг. Телефонное мошенничество (*УК-1-32)*
4. Дорожное яблоко. Троянские программы. Кви про кво (*УК-1-32)*
5. «Пляшущие свинки». Сбор информации из открытых источников. Способы повышения защиты от социальной инженерии (*УК-1-32)*

Раздел 3. Понятия криптографии. Симметричные криптосистемы

1. Основные понятия криптографии (*УК-1-34)*
2. Абсолютно устойчивые криптосистемы по Шеннону и Керкгоффса (*УК-1-34)*
3. Симметричные криптосистемы. Основные понятия (*УК-1-34)*
4. Классификация симметричных криптоалгоритмов (*УК-1-34)*
5. Шифр цезаря. Аффинный шифр (*УК-1-34)*
6. Одноразовые блокноты. Гаммирование (*УК-1-34)*
7. Блочные и поточные шифры. Основные понятия (*УК-1-34)*
8. Сеть Фейстеля (*УК-1-34)*
9. Алгоритм DES (*УК-1-34)*
10. Алгоритм МАГМА (*УК-1-34)*
11. Алгоритм Rijndael (*УК-1-34)*
12. Алгоритм RC4 (*УК-1-34)*

Раздел 4. Асимметричные криптосистемы.

1. Ассиметричные криптосистемы (*УК-1-34)*

2. Односторонние функции (*УК-1-34)*
3. Метод Эль-Гамаля (*УК-1-34)*
4. Метод RSA (*УК-1-34)*
5. Метод Диффи-Хелманна (*УК-1-34)*

Раздел 5. Электронная цифровая подпись и хэш-функции. Криптоанализ

1. Хэш-функции. Свойства. (*УК-1-34, УК-1-33)*
2. ЭЦП. Свойства (*УК-1-34, УК-1-33)*
3. «Хорошая» хэш-функция (*УК-1-34, УК-1-33)*
4. Основные понятия криптоанализа *(УК-1-34)*
5. Частотный анализ, метод полного перебора и метод встречи по середине (парадокс дней рождений) *(УК-1-34)*
6. Задачи факторизации и дискретного логарифмирования. *(УК-1-34)*
7. «Радужные таблицы» *(УК-1-34)*
8. «Соленый» хэш*(УК-1-34)*

Раздел 6. Блокчейн и криптовалюта

1. Понятие блокчейна (*УК-1-34, УК-1-33)*
2. Пример работы биткоина (*УК-1-34, УК-1-33)*
3. Майнинг в сети биткоин (*УК-1-34, УК-1-33)*
4. Преимущества и недостатки блокчейн технологий. Сфера использования (*УК-1-34, УК-1-33)*

Раздел 7. Идентификация и аутентификация

1. СКУД-системы. (*УК-1-33)*
2. Идентификация и аутентификация. (*УК-1-33)*
3. Штрих-коды и QR-коды. (*УК-1-33)*
4. RFID-метки. (*УК-1-33)*
5. Биометрические способы идентификации. Недостатки. (*УК-1-33)*
6. Виды аутентификации . (*УК-1-33)*
7. Touch Memory. Карты доступа. (*УК-1-33)*
8. Парольная аутентификация. . (*УК-1-33)*
9. Ошибки при использовании паролей. Многофакторная аутентификация. . (*УК-1-33)*
10. Одноразовые пароли. Повышения надежности парольной аутентификации. (*УК-1-33)*
11. СМАРТ-карты. Электронные ключи. (*УК-1-33)*

Раздел 8. Правовое регулирование информационной безопасности в РФ

1. Основные законы регулирующие защиту информации в РФ. (*УК-1-35)*
2. Роскомнадзор. ФСТЭК. Отдел «К» . (*УК-1-35)*

Перечень типовых задач для экзамена

(ОПК-3-У1, ОПК-3-У2 **)**

Задача 1: Зашифровать свое ФИО методом афинной системы Цезаря. Параметры b- № студента по списку, a- номер билета округленный до ближайшего взаимопростого числа с 33

Задача 2: Зашифровать свое ФИО методом одноразовых блокнотов

Задача 3: Зашифровать свое ФИО методом RSA. Параметры p- № студента по списку, q- номер билета. Оба числа округлить до ближайшего простого числа

Задача 4: Зашифровать свое ФИО методом Эль-Гамаля. Параметры p- № студента по списку, округленное до ближайшего простого числа

Задача 5: Зашифровать свое ФИО методом Хилла. Параметры A(определитель матрицы)- № студента по списку, округленный до ближайшего простого числа

Задача 6: Подписать свое ФИО ЭЦП RSA. Параметры p- № студента по списку, q- номер билета. Оба числа округлить до ближайшего простого числа

Перечень тестовых вопросов и заданий, используемых при устном опросе (текущий контроль успеваемости)

(*УК-1-31, УК-1-32, УК-1-33, УК-1-34, УК-1-35)*

1. ***(1 балл)*** К правовым методам, обеспечивающим информационную безопасность, относятся:
   a. Разработка аппаратных средств обеспечения правовых данных
   b. Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   c. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
2. ***(1 балл)*** Основными источниками угроз информационной безопасности являются все указанное в списке:
   a. Хищение жестких дисков, подключение к сети, инсайдерство
   b. Перехват данных, хищение данных, изменение архитектуры системы
   c. Хищение данных, подкуп системных администраторов, нарушение регламента работы
3. ***(1 балл)*** Виды информационной безопасности:
   a. Персональная, корпоративная, государственная
   b. Клиентская, серверная, сетевая
   c. Локальная, глобальная, смешанная
4. ***(1 балл)*** Цели информационной безопасности – своевременное обнаружение, предупреждение:
   a. несанкционированного доступа, воздействия в сети
   b. инсайдерства в организации

c. чрезвычайных ситуаций

5. ***(1 балл)*** Основные объекты информационной безопасности:
   a. Компьютерные сети, базы данных
   b. Информационные системы, психологическое состояние пользователей
   c. Бизнес-ориентированные, коммерческие системы
6. ***(1 балл)*** Основными рисками информационной безопасности являются:
   a. Искажение, уменьшение объема, перекодировка информации
   b. Техническое вмешательство, выведение из строя оборудования сети
   c. Потеря, искажение, утечка информации
7. ***(1 балл)*** К основным принципам обеспечения информационной безопасности относится:
   a. Экономической эффективности системы безопасности
   b. Многоплатформенной реализации системы
   c. Усиления защищенности всех звеньев системы
8. ***(1 балл)*** Основными субъектами информационной безопасности являются:
   a. руководители, менеджеры, администраторы компаний
   b. органы права, государства, бизнеса
   c. сетевые базы данных, фаерволлы
9. ***(1 балл)*** К основным функциям системы безопасности можно отнести все перечисленное:
   a. Установление регламента, аудит системы, выявление рисков
   b. Установка новых офисных приложений, смена хостинг-компании
   c. Внедрение аутентификации, проверки контактных данных пользователей
10. ***(1 балл)*** Принципом информационной безопасности является принцип недопущения:
    a. Неоправданных ограничений при работе в сети (системе)
    b. Рисков безопасности сети, системы
    c. Презумпции секретности
11. ***(1 балл)*** Принципом политики информационной безопасности является принцип:
    a. Невозможности миновать защитные средства сети (системы)
    b. Усиления основного звена сети, системы
    c. Полного блокирования доступа при риск-ситуациях
12. ***(1 балл)*** Принципом политики информационной безопасности является принцип:
    a. Усиления защищенности самого незащищенного звена сети (системы)
    b. Перехода в безопасное состояние работы сети, системы
    c. Полного доступа пользователей ко всем ресурсам сети, системы
13. ***(1 балл)*** Принципом политики информационной безопасности является принцип:
    a. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
    b. Одноуровневой защиты сети, системы
    c. Совместимых, однотипных программно-технических средств сети, системы
14. ***(1 балл)*** К основным типам средств воздействия на компьютерную сеть относится:
    a. Компьютерный сбой
    b. Логические закладки («мины»)
    c. Аварийное отключение питания
15. ***(1 балл)*** Когда получен спам по e-mail с приложенным файлом, следует:
    a. Прочитать приложение, если оно не содержит ничего ценного – удалить
    b. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
    c. Удалить письмо с приложением, не раскрывая (не читая) его
16. ***(1 балл)*** Принцип Кирхгофа:
    a. Секретность ключа определена секретностью открытого сообщения
    b. Секретность информации определена скоростью передачи данных
    c. Секретность закрытого сообщения определяется секретностью ключа
17. ***(1 балл)*** ЭЦП – это:
    a. Электронно-цифровой преобразователь
    b. Электронно-цифровая подпись
    c. Электронно-цифровой процессор
18. ***(1 балл)*** Наиболее распространены угрозы информационной безопасности корпоративной системы:
    a. Покупка нелицензионного ПО
    b. Ошибки эксплуатации и неумышленного изменения режима работы системы
    c. Сознательного внедрения сетевых вирусов
19. ***(1 балл)*** Наиболее распространены угрозы информационной безопасности сети:
    a. Распределенный доступ клиент, отказ оборудования
    b. Моральный износ сети, инсайдерство
    c. Сбой (отказ) оборудования, нелегальное копирование данных
20. ***(1 балл)*** Наиболее распространены средства воздействия на сеть офиса:
    a. Слабый трафик, информационный обман, вирусы в интернет
    b. Вирусы в сети, логические мины (закладки), информационный перехват
    c. Компьютерные сбои, изменение администрирования, топологии
21. ***(1 балл)*** Утечкой информации в системе называется ситуация, характеризуемая:
    a. Потерей данных в системе
    b. Изменением формы информации
    c. Изменением содержания информации
22. ***(1 балл)*** Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
    a. Целостность
    b. Доступность
    c. Актуальность
23. ***(1 балл)*** Угроза информационной системе (компьютерной сети) – это:
    a. Вероятное событие
    b. Детерминированное (всегда определенное) событие
    c. Событие, происходящее периодически
24. ***(1 балл)*** Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
    a. Регламентированной
    b. Правовой
    c. Защищаемой
25. ***(1 балл)*** Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
    a. Программные, технические, организационные, технологические
    b. Серверные, клиентские, спутниковые, наземные
    c. Личные, корпоративные, социальные, национальные
26. ***(1 балл)*** Окончательно, ответственность за защищенность данных в компьютерной сети несет:
    a. Владелец сети
    b. Администратор сети
    c. Пользователь сети

27. ***(1 балл)*** Политика безопасности в системе (сети) – это комплекс:
    a. Руководств, требований обеспечения необходимого уровня безопасности
    b. Инструкций, алгоритмов поведения пользователя в сети
    c. Нормы информационного права, соблюдаемые в сети
28. ***(1 балл)*** Наиболее важным при реализации защитных мер политики безопасности является:
    a. Аудит, анализ затрат на проведение защитных мер
    b. Аудит, анализ безопасности
    c. Аудит, анализ уязвимостей, риск-ситуаций
29. ***(1 балл)*** Основная масса угроз информационной безопасности приходится на:
    а) Троянские программы
    б) Шпионские программы
    в) Черви
30. ***(1 балл)*** Какой вид идентификации и аутентификации получил наибольшее распространение:
    а) системы PKI
    б) постоянные пароли
    в) одноразовые пароли
31. ***(1 балл)*** Под какие системы распространение вирусов происходит наиболее динамично:
    а) Windows
    б) Mac OS
    в) Android
32. ***(1 балл)*** Заключительным этапом построения системы защиты является:
    а) сопровождение
    б) планирование
    в) анализ уязвимых мест
33. ***(1 балл)*** Какие угрозы безопасности информации являются преднамеренными:
    а) ошибки персонала
    б) открытие электронного письма, содержащего вирус
    в) не авторизованный доступ
34. ***(1 балл)*** Какой подход к обеспечению безопасности имеет место:
    а) теоретический
    б) комплексный
    в) логический
35. ***(1 балл)*** Системой криптографической защиты информации является:
    а) BFox Pro
    б) CAudit Pro
    в) Крипто Про
36. ***(1 балл)*** Какие вирусы активизируются в самом начале работы с операционной системой:
    а) загрузочные вирусы
    б) троянцы
    в) черви
37. ***(1 балл)*** Stuxnet – это:
    а) троянская программа
    б) макровирус
    в) промышленный вирус
38. ***(1 балл)*** Таргетированная атака – это:
    а) атака на сетевое оборудование
    б) атака на компьютерную систему крупного предприятия
    в) атака на конкретный компьютер пользователя
39. ***(1 балл)*** Под информационной безопасностью понимается:
    а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
    б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
    в) нет верного ответа
40. ***(1 балл)*** Защита информации:
    а) небольшая программа для выполнения определенной задачи
    б) комплекс мероприятий, направленных на обеспечение информационной безопасности
41. ***(1 балл)*** Информационная безопасность зависит от:
    а) компьютеров, поддерживающей инфраструктуры
    б) пользователей
    в) информации
42. ***(1 балл)*** Конфиденциальностью называется:
    а) защита программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
    б) описание процедур
    в) защита от несанкционированного доступа к информации
43. ***(1 балл)*** Для чего создаются информационные системы:
    а) получения определенных информационных услуг
    б) обработки информации
    в) оба варианта верны
44. ***(1 балл)*** Кто является основным ответственным за определение уровня классификации информации:
    а) руководитель среднего звена
    б) владелец
    в) высшее руководство
45. ***(1 балл)*** Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
    а) хакеры
    б) контрагенты
    в) сотрудники
46. ***(1 балл)*** Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству:
    а) снизить уровень классификации этой информации
    б) улучшить контроль за безопасностью этой информации
    в) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
47. ***(1 балл)*** Что самое главное должно продумать руководство при классификации данных:
    а) управление доступом, которое должно защищать данные
    б) оценить уровень риска и отменить контрмеры
    в) необходимый уровень доступности, целостности и конфиденциальности
48. ***(1 балл)*** Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
    а) владельцы данных

б) руководство
в) администраторы

49. ***(1 балл)*** Процедурой называется:
а) пошаговая инструкция по выполнению задачи
б) обязательные действия
в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

50. ***(1 балл)*** Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании:
а) проведение тренингов по безопасности для всех сотрудников
б) поддержка высшего руководства
в) эффективные защитные меры и методы их внедрения

51. ***(1 балл)*** Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков:
а) когда риски не могут быть приняты во внимание по политическим соображениям
б) для обеспечения хорошей безопасности нужно учитывать и снижать все риски
в) когда стоимость контрмер превышает ценность актива и потенциальные потери

52. ***(1 балл)*** Что такое политика безопасности:
а) детализированные документы по обработке инцидентов безопасности
б) широкие, высокоуровневые заявления руководства
в) общие руководящие требования по достижению определенного уровня безопасности

53. ***(1 балл)*** Какая из приведенных техник является самой важной при выборе конкретных защитных мер:
а) анализ рисков
б) результаты ALE
в) анализ затрат / выгоды

54. ***(1 балл)*** Что лучше всего описывает цель расчета ALE:
а) количественно оценить уровень безопасности среды
б) оценить потенциальные потери от угрозы в год +
в) количественно оценить уровень безопасности среды

55. ***(1 балл)*** Тактическое планирование:
а) среднесрочное планирование
б) ежедневное планирование
в) долгосрочное планирование

56. ***(1 балл)*** Эффективная программа безопасности требует сбалансированного применения:
а) контрмер и защитных механизмов
б) процедур безопасности и шифрования
в) технических и нетехнических методов

57. ***(1 балл)*** Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
а) уровень доверия, обеспечиваемый механизмом безопасности
б) внедрение управления механизмами безопасности
в) классификацию данных после внедрения механизмов безопасности

58. ***(1 балл)*** Что из перечисленного не является целью проведения анализа рисков:
а) выявление рисков
б) делегирование полномочий
в) количественная оценка воздействия потенциальных угроз

5.2. Перечень работ, выполняемых по дисциплине

По дисциплине предусмотрено: выполнение 2 домашних заданий

Домашние задания

1. Реализация алгоритма RC42. (УК-1-З4, ОПК-3-В1,ОПК-3-В1)
2. Частотный анализ во взломе шифров (УК-1-З4, ОПК-3-У1,,ОПК-3-В1)

Домашние задания включают в себя ряд типовых задач с индивидуальными вариантами

Пример домашнего задания (ДЗ)

1. Зашифровать алгоритмом RC4 свое ФИО. Параметр N в алгоритме брать не менее 16.
2. Произвести взлом следующего шифра методом частотного анализа:

ю эмц ъш июг-бъв фпм сшлкивюх сшъьюр лэмьмг пмдцюьютъмпм дхищичфпм, цмц дммкчшх, тцм фпм нмцёц эювфцо вэмф зищтюь. смпшъ ямгмдюхдё ъш смлшхю ю зъмпмлъштюцфхоъм инзьхоьихдё. ксщцоё лшпхмцюхю ъшщюэги. гшгмэм щф кьхм фпм ивюэхфъюф, гмпвш пмдцёзю мгшлшхюдо дмэдфз ъфлъшгмзьф фзи хувю. эфсъфф, ъфлъшгмзафз кьх цмхогм мвюъ. смпшъ ямтцю дсшли илъшх бцмпм эьдмгмпм пмдямвюъш. шсцис кфрхю, мыюафс шзфсюгшъдгмр сшлэфвгю, гмцмсьр вфэёцо хфц ъшлшв вмясшеюэшх смпшъш м цмз, тцм ясмюднмвюхм д ъюз э зуънфъдгмз вэмсаф ясшэмдивюё, ш ямцмз ясмдюх мямлъщцо ямвмлсфэшфзьн э эмфъъьн ясфдцияхфъюён. кфрхю юлитшучфф ю нмхмвъм дзмцсфх ъш смпшъш, ямцмз ямгшлшх фзи дэмф ивмдцмэфсфъюф.
— цмхогм тцм юлитшх эшеф вмдоф, зюдцфс смпшъ, — дгшлшх кфрхю. — эь дмэдфз ъф ямнмщю ъш тфхмэфгш ъш цмр дцшсмр ымцмпсшыюю. эяфсэьф иэювфэ дъмэш, ё ясмдцм эшд ъф илъшх.
— гмпвш бцм кьхм? — дясмдюх смпшъ.
— ъфвфху цмзи ъшлшв, ъш шэцмдфсэюдф и ксшцофэ ысфрдхюъпмэ, — мцэфцюх кфрхю. цояютъьр ясфвдцшэюцфхо дсфвъфпм лшяшвш, дцмхо ншсшгцфсъьр ъфзъмпм пьидшэьр шзфсюгшъдгюр шгафъц, вш ю мвфщвш ю зштъфсш вфсщшцодё цмщф цояютъм шзфсюгшъдгюф. смпшъ ивюэюхдё: гшг бцм мъ ъф лшзфцюх кфрхю ъш шэцмлшясшэгф?
кфрхю вмксмвиеъм ихькъихдё:
— зь дтюцшфз, тцм ксщцоё ысфрдхюъпю ёэхёуцдё эмдцмтъмпфсзшъдгюзю шпфъцшзю, бцм ямзюзм эдфпм ясмтфпм. кфддмэфдцъьф ю шхтъьф, щихюгмэшцьф вфхоаь. ш ямцмз эвсип цшз ямёэхёфцфдо эь ю лшэмвюцф д ъюзю всищки. ъи ю зь, фдцфдцэфъъм, дцшхю эшд ясмэфсёцо. ямлэмъюхю э эшеюъпцмъ, эьёдъюхю ъшдтфц эшеюн эюл ю ясмтфф. ш ямцмз ё дцшх юлитшщо эшеф хютъмф вфхм. ю циц эдяхьхм гмф-тцм фчф, ю ё лшцсфкмэшх зфдцъьф пшлфць, эьефвеюф лш эсфзё эшефпм ясфкьэшъюё э шэдцсюю ю пфсзшъюю. ю эдф дмехмдо. эшз ившхмдо эьдхфвюцо цфн дфзфсьн цюямэ юл зуънфъш, ю эмц цфяфсо эь эфсъихюдо дувш, тцмкь ямикюэшцо юн эдфн. икюрдцэм змхоцгф э эфъф, лшцфз — гшсхш яышъш э пшзкиспф. ш дхфвиучюф э эшефз дяюдгф ксшцоё ысфрдхюъпю, ё ъф меюкдё?
— ё ясюфншх дувш ясмвшэшцо гмзяоуцфсь, — идцшхм ю сшлвсшщфъъм мцэфцюх смпшъ. — бцм эдф.
кфрхю ямщшх яхфтшзю.
— зъф ъфэшщъм, тфз эь лвфдо лшъюзшфцфдо. ъф иямхъмзмтфъ дцмёцо ъш дцсшщф лшгмъъмддцю э бцмр дцсшъф. ъм нмти ясфвиясфвюцо: сигю ясмто мц ысфрдхюъпмэ. ъф дзфрцф юн цсмпшщо. дхюегмз зъмпм эсфзфъю ё ямцсшщюх ъш дхфщги лш ъюзю ю сшлсшкмцги, тцмкь сшлмкхштюцо фчф мвъм еяюмъдгмф пъфлвм эмддцмтъмр пфсзшъюю. гмсмтф, икюцо юн ё эшз ъф ямлэмху, ъф нмти, тцмкь мкмсэшхдё дхфв.
ю циц эвсип смпшъ ямъёх, ямтфзи ксшцоё ысфрдхюъпю кьхю цшг д ъюз хукфлъь ю всищфхукъь.
— юн юъцфсфдиуц змю ъмэьф гмзяоуцфсъьф сшлсшкмцгю? — дясмдюх мъ кфрхю.
— ъютицо ъф ивюэхудо, фдхю бцм цшг, — мцэфщюх цмц. — гмзяоуцфсь — мдмкфъъм ъмэьф — ъшнмвёцдё ямв лшясфцмз э гмззиъюдцютфдгюн дцсшъшн. ъм ю бцм зфъё цмщф зшхм кфдямгмюц. ямдгмхоги ё лъшу, тфз эь дмкюсшфцфдо ъшпсшвюцо бцюн цюямэ. фчф сшл ясфвиясфщвшу: цмхогм ямясмкирцф ю дцшъфцф змюз эсшпмз. смпшъ дзмцсфх ъш ъфпм нмхмвъм ю ясюдцшхоъм.
— ъф ямъюзшу, м тфз бцм эь, ъм ямлэмхоцф ю зъф вшцо дмэфц. ъф дцшъмэюцфдо и зфъё ъш яицю, юъштф сшлвшэху. ю ямцмз, ъютфпм эь дм зъмр ъф двфхшфцф. ъю тфсцш! и зфъё нмсмеюф дэёлю э яфъцшпмъф. ю вхё ъюн змю гмзяоуцфсь гивш гшг эшщъфр, ъфщфхю эдё цш тиео, гмцмсиу эь дмкюсшфцфдо эьивюцо и бцюн цшг ъшльэшфзьн гсшдъьн еяюмъмэ. цмщф зъф, пъфлвм сшлмкхштюхю юл вэин ясювисгмэ!
кфрхю мгюъих фпм лшвизтюэьз элпхёвмз, лшцфз дгшлшх:

— хшвъм, эшд зь ъф цсмъфз, ъм гшг ъшдтфц ямвсищгю? — ю мъ гюэгмз игшлшх ъш смлшхю, дювфэеиу ъш вюэшъф. — ищ зь-цм дизффз вмдцшэюцо бцмр гигмхгф

ъфеицмтъьф ъфясюёцъмдцю. мвюъ, эдфпм мвюъ цфхфымъъьр лэмъмг, ю эь фф ъюгмпвш кмхоеф ъф иэювюцф

Перечень вопросов к домашним заданиям

(УК-1-З1, УК-1-З2, УК-1-З3, УК-1-З4)

1. Что такое симметричный криптоалгоритм?
2. Какие вы знаете симметричные шифры?
3. Что такое открытый и закрытый ключ?
4. Что такое мод N?
5. Опишите, для чего используется расширенный алгоритм Евклида
6. Чем отличается аффинный шифр от шифра Цезаря, что у них общего?
7. Как хранятся пароли в различных операционных системах?
8. Что такое хэш-функция
9. Что такое ЭЦП?
10. Чем отличается хэш-функция от ЭЦП?
11. Современные симметричные шифры
12. Особенность шифра RC4
13. Что такое «парадокс дней рождений»
14. Частотный анализ
15. Недостатки частного анализа
16. Факторизация
17. «Соль» к хэшу
18. Радужные таблицы
19. Проблемы вычислительной сложности в шифровании и криптоанализе
20. Абсолютно устойчивый шифр

5.3. Оценочные материалы, используемые для экзамена (описание билетов, тестов и т.п.)

Экзаменационный билет включает в себя фундаментальный теоретический вопрос и прикладной теоретический вопрос из установленного перечня контрольных вопросов, используемых при формировании экзаменационных билетов при оценке знаний обучающихся на экзамене по темам, изложенным в разделах 1-8 данной РПД, а также практическое задание из установленного перечня контрольных заданий, используемых при формировании экзаменационных билетов при оценке знаний обучающихся на экзамене по темам, изложенным в разделах 3, 4, 5 данной РПД.

Пример экзаменационного билета:

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»
Кафедра «Автоматизированных и информационных систем управления»
13.03.02 Электроэнергетика и электротехника
Профиль – Электропривод и автоматика
Дисциплина «Защита информации»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Touch Memory. Карты доступа
2. Роскомнадзор. ФСТЭК. Отдел «К».

3. Зашифровать свое ФИО методом RSA. Параметры p- № студента по списку, q- номер билета. Оба числа округлить до ближайшего простого числа

Экзаменатор _____ О.Ф.Козырь

Утверждено на заседании кафедры АИСУ

Протоколом №___ от _____ 2023 г.

Заведующий кафедрой АИСУ _____ Д.А. Полещенко

Билеты в бумажном виде хранятся на кафедре АИСУ и утверждены ее заведующим (или заместителем зав. кафедрой).

5.4. Методика оценки освоения дисциплины

№ п/п	Вид оценочного средства	Критерий	Оценка
1	Выполнение и защита домашних заданий	Все задачи домашнего задания выполнены без ошибок, либо с непринципиальными ошибками, не влияющими на физическую суть результата	«Зачтено»

			Задание не выполнено полностью, либо выполнены не все задачи, либо в решении допущены существенные ошибки, неисправленные после собеседования с преподавателем	«Не зачтено»	
	2	Экзамен	Компетенции сформированы. Обучающийся демонстрирует: - глубокие знания содержания изученной дисциплины во взаимосвязи с другими дисциплинами; - способность использовать теоретические знания при выполнении практических заданий; - аргументированные, исчерпывающие ответы на все вопросы по билету, а также дополнительные вопросы экзаменатора; - умение выполнять и обосновывать решение практических заданий высокого уровня сложности; - наличие собственной обоснованной позиции по обсуждаемым вопросам; - свободное использование в ответах на вопросы материалов рекомендованной основной и дополнительной литературы.	«Отлично»	
			Компетенции сформированы. Обучающийся демонстрирует: - знание основных терминов по содержанию изученной дисциплины; - твердые знания теоретического материала; - умение дать четкие ответы на поставленные вопросы; - умение решать практические задания; - владение основной литературой, рекомендованной программой дисциплины. Допускаются незначительные неточности в ответах на теоретические вопросы и при выполнении практических заданий.	«Хорошо»	
			Компетенции сформированы. Обучающийся демонстрирует: - знания теоретического материала по изученной дисциплине; - неполные ответы на основные вопросы, допуская ошибки в ответе; недостаточное понимание сущности излагаемых вопросов; - неточные ответы на дополнительные вопросы; - умение выполнять практические задания без грубых ошибок; - недостаточное владение литературой, рекомендованной программой дисциплины.	«Удовлетворительно»	
			Компетенции не сформированы. Обучающийся демонстрирует: - существенные пробелы в знаниях учебного материала; - принципиальные ошибки при ответе на основные вопросы билета, отсутствие знаний и понимания основных терминов и определений; - непонимание сущности дополнительных вопросов в рамках заданий билета; - отсутствие навыка или существенные ошибки при выполнении практических заданий; - незнание литературы, рекомендованной программой дисциплины.	«Неудовлетворительно»	

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ				
6.1. Рекомендуемая литература				
6.1.1. Основная литература				
Обозначение	**Авторы, составители**	**Заглавие**	**Библиотека**	**Издательство, год**

Л 1.1	Загинайлов, Ю.Н	Теория информационной безопасности и методология защиты информации : учебное пособие	ЭБС «Университетская библиотека онлайн» URL: http://biblioclub.ru/index.php?page=book&id=276557	Москва ; Берлин : Директ-Медиа, 2015
Л 1.2	Прохорова О.В.	Информационная безопасность и защита информации : учебник	ЭБС «Университетская библиотека онлайн» URL: http://biblioclub.ru/index.php?page=book&id=438331	Самара : Самарский государственный архитектурно-строительный университет, 2014
Л 1.3	Черняков М. В, Петрушин А. С.	Основы информационных технологий	НТБ СТИ НИТУ «МИСИС»	М : ИКЦ "Академкнига", 2007
6.1.2. Дополнительная литература				
Обозначение	**Авторы, составители**	**Заглавие**	**Библиотека**	**Издательство, год**
Л 2.1	Сергеева, Ю.С..	Защита информации: Конспект лекций	ЭБС «Университетская библиотека онлайн» URL: http://biblioclub.ru/index.php?page=book&id=72670	Москва: А-Приор, 2011
Л 2.2	В. И. Аверченков, М. Ю. Рытов, Г. В. Кондрашин, М. В. Рудановский	Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов	ЭБС «Университетская библиотека онлайн» URL: http://biblioclub.ru/index.php?page=book&id=93351	М. : Флинта, 2016
6.1.3. Методические разработки				
Обозначение	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л 3.1	Соловьев А.Ю.	Конспект лекций по курсу «Защита информации»	НТБ СТИ НИТУ «МИСИС»	Старый Оскол, СТИ НИТУ «МИСиС», 2018
Л 3.2	Соловьев А.Ю	Пособие к выполнению практических занятий по курсу «Защита информации»	НТБ СТИ НИТУ «МИСИС»	Старый Оскол, СТИ НИТУ «МИСиС», 2018
Л 3.3	Соловьев А.Ю	Пособие к выполнению домашних заданий по курсу «Защита информации»	НТБ СТИ НИТУ «МИСИС»	Старый Оскол, СТИ НИТУ «МИСиС», 2020
6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»				
Э 1	Бесплатная электронная библиотека онлайн «Единое окно к образовательным ресурсам» [Электронный ресурс]: http://window.edu.ru			
Э 2	Открытое образование [Электронный ресурс]: https://openedu.ru/			
Э 3	LMS Canvas [Электронный ресурс]: https://lms.misis.ru			
6.3. Перечень программного обеспечения				
П 1	Microsoft Windows			
П 2	Microsoft Office			
6.4. Перечень информационных справочных систем и профессиональных баз данных				

И 1	eLIBRARY.RU - НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА [Электронный ресурс]: https://elibrary.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ	
7.1	**Аудитория №419** **«Лекционная аудитория»** Перечень основного оборудования, учебно-наглядных пособий: • Усилитель-распределитель • Монитор • Панель аудио • Монитор планшетный • Компьютер • Настенный экран • Микшерный пульт • Мультимедиа проектор • Усилитель звука • Документ -камера • Система видео-конференц связи • Контроллер • Коммутатор • Звуковые колонки • Вокальная радиосистема • Комплект учебной мебели на 70 посадочных мест
7.2	**Аудитория №406** **«Лаборатория прикладного программирования»** Перечень основного оборудования, учебно-наглядных пособий: • Монитор - 9шт. • Персональный компьютер - 9шт. • Проектор • Экран настенный • Усилитель-распределитель • Комплект учебной мебели на 25 посадочных мест.
7.3	**Аудитория №306** **«Кабинет для самостоятельной работы»** Перечень основного оборудования, учебно-наглядных пособий: • проектор; • доска; • экран настенный; • компьютер – 6 шт.; • комплект учебной мебели на 20 человек. В помещении для самостоятельной работы обучающихся имеется подключение к сети «Интернет» и доступ в электронную информационно-образовательную среду организации.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ
Промежуточная аттестация по дисциплине предусмотрена в виде экзамена. Обучение проводится в один семестр и организуется в соответствии с настоящей программой. Самостоятельная работа студентов осуществляется и контролируется с помощью: – сдачи домашних заданий, Экзамен проставляется при условии выполнения учебного плана дисциплины, и по результатам ответов на экзаменационные билеты