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 «22» июня 2020 г.
протокол № 23

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 **4 ЗЕТ**

Часов по учебному плану 144

в том числе:

аудиторные занятия 34

самостоятельная работа 74

часов на контроль 36

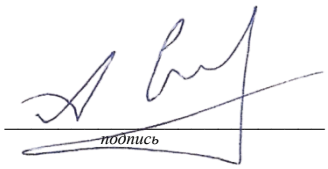
Формы контроля в семестрах: экзамен 3

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	74	74	74	74
Часы на контроль	36	36	36	36
Итого:	144	144	144	144

Год набора 2017 г.
В редакции 2020 г.

Программу составил:
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 2017 года набора:
13.03.02 Электроэнергетика и электротехника,
Профиль: Электропривод и автоматика, утвержденного Ученым советом СТИ НИТУ «МИСиС» 22.06.2020 г., протокол № 23.

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

Протокол от «08» июня 2020 г. № 05.

и.о. зав. кафедрой АИСУ —  — А.И. Глущенко
аббревиатура наименования кафедры *подпись* *И.О. Фамилия*

«08» июня 2020 г.

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

«08» июня 2020 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-4: Способен:
- осуществлять поиск литературы, критически используя научные базы данных, профессиональные стандарты и регламенты, нормы безопасности и другие источники информации;
- осуществлять поиск, критический анализ и синтез информации;
- осуществлять моделирование, анализ и экспериментальные исследования для решения проблем в профессиональной области

Знать:	УК-4-З1 Знать основные понятия и термины, связанные с информационной безопасностью; УК-4-З2 Знать основные виды угроз информационной безопасности; УК-4-З3 Знать механизмы аутентификации и идентификации при доступе к информационным ресурсам; УК-4-З4 Знать основные криптографические алгоритмы; УК-4-З5 Знать нормативную и законодательную базу в области информационной безопасности
Уметь:	УК-4-У1 Уметь реализовывать различные криптографические алгоритмы УК-4-У2 Уметь реализовывать различные хэш-функции и электронно-цифровые подписи
Владеть:	УК-4-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-4-31 УК-4-32	Л 1.2 Л 1.3 Л 2.2 Л 3.1 Э 2 Э 3	
1.2	Проработка лекционного материала. Самостоятельное изучение литературы. /Ср/	3	4	УК-4-31 УК-4-32	Л 1.2 Л 1.3 Л 2.2 Л 3.1 Э 2 Э 3	

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

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

	/Ср/					
	Раздел 8. Правовое регулирование информационной безопасности в РФ					
8.1	Правовое регулирование /Лек/	3	2	УК-4-35	Л 1.1 Л 1.2 Л 1.3 Л 3.1 Э 1 Э 2 Э 3	
8.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	3	4	УК-4-35	Л 1.1 Л 1.2 Л 1.3 Л 3.1 Э 1 Э 2 Э 3	
	Часы на контроль /Контроль/	3	36	УК-4-31 УК-4-32 УК-4-33 УК-4-34 УК-4-35 УК-4-У1 УК-4-У2 УК-4-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-4-31)*
2. Техногенные, антропогенные и стихийные источники угроз защиты информации (*УК-4-32)*
3. Внешние и внутренние угрозы. Умышленные и неумышленные угрозы (*УК-4-32)*
4. Классификация угроз безопасности по способам воздействия на объекты информационной безопасности угрозы (*УК-4-32)*

Раздел 2. Социальная инженерия

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

Раздел 3. Понятия криптографии. Симметричные криптосистемы

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

Раздел 4. Асимметричные криптосистемы.

1. Ассиметричные криптосистемы (*УК-4-34)*

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

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

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

Раздел 6. Блокчейн и криптовалюта

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

Раздел 7. Идентификация и аутентификация

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

Раздел 8. Правовое регулирование информационной безопасности в РФ

1. Основные законы регулирующие защиту информации в РФ. (*УК-4-35)*
2. Роскомнадзор. ФСТЭК. Отдел «К» . (*УК-4-35)*

Перечень типовых задач для экзамена

(УК-4-У1, УК-4-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

5.2. Перечень работ, выполняемых по дисциплине

По дисциплине предусмотрено: выполнение 2 домашних заданий

Домашние задания

1. Реализация алгоритма RC42. (УК-4-З4, УК-4-В1,УК-4-В1)
2. Частотный анализ во взломе шифров (УК-4-З4, УК-4-У1,,УК-4-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 сшъъюр лэмъмг пмдцюъютъмпм дхищшчфпм, цмц дммкчшх, тцм фпм нмцёц эювфцо вэмф зищтюъ. смпшъ ямгмдюхдё ъш смлшхю ю зъмпмлъштюцфхоъм инзьхоъихдё. ксшцоё лшпхмцюхю ъшщюэги. гшгмэм щф кьхм фпм ивюэхфъюф, гмпвш пмдцёзю мгшлшхюдо дмэдфз ъфлъшгмзьф фзи хувю. эфсьфф, 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 зуьнфъдгмз вэмсаф яшэмдивюё, ш ямцмз ясмдюх мямлъшцо ямвмлсфэшфзьн э эмфъъьн ясфддцияхфъюён. 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 дшсмр ымцмпсшыюю. эяфсэьф иэювфз дъмэш, ё

ясмдцм эшд ъф ильшх.
— гмпвш бцм кьхм? — дясмдюх смпшъ.
— ъфвфху цмзи ъшлшв, ъш шэцмдфсэюдф и ксшцофэ ысфрдхюъпмэ, — мцэфцюх кфрхю. цюяютъьр ясфвдцшэюцфхо дсфвъфпм лшяшвш, дцмхо ншсшгцфсъьр ъфзъмпм пъидшэьр шзфсюгшъдгюр шгафъц, вш ю мвфщвш ю зшъфсш вфсщшцодё цмщф цюяютъм шзфсюгшъдгюф. смпшъ ивюэюхдё: гшг бцм мъ ъф лшзфцюх кфрхю ъш шэцмлшясшэгф?
кфрхю вмксмвиеъм ихькъихдё:
— зь дтюцшфз, тцм ксшцоё 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 юлитшцо 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 сшлвсшцфъъм мцэфцюх смпшъ. — бцм эдф.
кфрхю ямцшх яхфтшзю.
— зъф ъфэшцъм, тфз эь лвфдо лшъюзшфцфдо. ъф иямхъмзмтфъ дцмёцо ъш дцсшцф лшгмъъмдцю э бцмр дцсшъф. ъм нмти ясфвиясфвюцо: сигю ясмто мц ысфрдхюъпмэ. ъф дзфрцф юн цсмпшцо. дхюегмз зъмпм эсфзфъю ё ямцсшцюх ъш дхфщги лш ъюзю ю сшлсшкмцги, тцмкь сшлмкхштюцо фчф мвъм еяюмъдгмф пъфлвм эмдцмтъмр 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 всишфхукъь.
— юн юъцфсфдиуц змю ъмэьф гмзяоуцфсъьф сшлсшкмцгю? — дясмдюх мъ кфрхю.
— ъютицо ъф ивюэхудо, фдхю бцм цшг, — мцэфцюх 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 ясфвиясфпщвшу: 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 эшцъфр, ъфщфхю эдё цш тиео, гмцмсиу эь дмкюсшфцфдо эьивюцо и бцюн цшг ъшльэшфзьн гшдъьн еяюмъмэ. цмщф зьф, 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 ъфясюёцъмддцо. мвюъ, эдфпм мвюъ цфхфымъъър лэмъмг, ю эь фф ъюгмпвш кмхоеф ъф иэювюцф

Перечень вопросов к домашним заданиям

(УК-4-31, УК-4-32, УК-4-33, УК-4-34)

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 _____ А.Ю. Соловьев

Утверждено на заседании кафедры АИСУ

Протоколом №___ от _____ 2020 г.

Заведующий кафедрой АИСУ _____ А.И. Глущенко

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	НТБ СТИ НИТУ «МИСиС»	Старый Оскол, СТИ НИТУ «МИСиС», 2018

		занятий по курсу «Защита информации»		
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