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

Информационная безопасность

Закреплена за кафедрой	**Кафедра автоматизированных и информационных систем управления**
Направление подготовки	09.03.02 Информационные системы и технологии
Профиль	Информационные системы и технологии
Квалификация	**Бакалавр**
Форма обучения	**Очная**
Общая трудоемкость	**4 ЗЕТ**

Часов по учебному плану	144
в том числе:	
аудиторные занятия	51
самостоятельная работа	57
часов на контроль	36

Формы контроля в семестрах:
экзамен 7, курсовая работа 8

Распределение часов дисциплины по семестрам

Семестр	7		8		Итого	
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	17	17	-	-	17	17
Лабораторные	17	17	-	-	17	17
Практические	17	17	-	-	17	17
Контактная работа	51	51	-	-	51	51
Сам. работа	21	21	36	36	57	57
Часы на контроль	36	36	-		36	36
Итого	108	108	36	36	144	144

Год набора 2020 г.
В редакции 2023г.

Программу составил:
доцент каф. АИСУ, кандидат технических наук
Соловьев Антон Юрьевич

Должность,уч.ст., уч.зв ФИО полностью *подпись*

Рабочая программа дисциплины

Информационная безопасность

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 09.03.02 Информационные системы и технологии (приказ от 05.03.2020 г. № 95 о.в.)

Составлена на основании учебного плана 2020 года набора.

09.03.02 Информационные системы и технологии,
Профиль: Информационные системы и технологии, утвержденного Ученым советом СТИ НИТУ «МИСИС» 22.06.2020 г., протокол № 23.

Рабочая программа одобрена на заседании кафедры Автоматизированных и информационных систем управления

Протокол от «24» мая 2023 г. № 3

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. каф. АИСУ, кандидат технических наук, доцент — Д.А. Полещенко
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	
Часть ОПОП ВО	Б1.О
2.1	**Требования к предварительной подготовке обучающихся – предшествующие дисциплины**
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	Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты

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;
Уметь:	УК-4-У1 – Уметь определять и классифицировать угрозы и атаки.
Владеть:	УК-4-В1 – Владеть навыками обнаружения уязвимостей веб-ресурсов
ОПК-3 **Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности**	
Знать:	ОПК-4-З1– Знать нормативную и законодательную базу в области информационной безопасности
Уметь:	ОПК-4-У1 – Уметь проводить анализ защищенности информационных объектов в различных сферах деятельности человека;
Владеть:	ОПК-4-В1– Владеть навыками реализации поиска потенциально компрометирующей информации в интернете
ПК-1 Способен участвовать в работах по: **- доводке и освоению информационных технологий в ходе внедрения и эксплуатации информационных технологий;** **- поддержанию работоспособности информационных систем и технологий в заданных функциональных характеристиках и в соответствии с критериями качества;** **- управлению программно-аппаратными средствами информационных служб инфокоммуникационной системы**	

организации; - обеспечению безопасности и целостности данных информационных систем и технологий, а также условий жизненного цикла информационных систем; - адаптации приложений к изменяющимся условиям функционирования; - администрированию сетевой подсистемы инфокоммуникационной системы организации. Использовать технологии разработки объектов профессиональной деятельности в различных областях.	
Знать:	ПК-1-З1 – Знать механизмы аутентификации и идентификации при доступе к информационным ресурсам; ПК-1-З2 – Знать основные криптографические алгоритмы; ПК-1-З3- Знать основные веб-уязвимости и веб-атаки
Уметь:	ПК-1-У1 – Уметь проводить анализ устойчивости различных криптографических алгоритмов ПК-1-У2 – Уметь проводить анализ устойчивости хешей паролей пользователей
Владеть:	ПК-1-В1 – Владеть навыками реализации различных криптографических алгоритмов ПК-1-В2– Владеть навыками реализации различных хэш-функций и электронно-цифровых подписей ПК-1-В3– Владеть навыками реализации защиты от веб-угроз

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/	7	2	УК-4-З1 УК-4-З2	Л 1.2 Л 1.3 Л 2.2 Э 2 Э 3	
1.2	Проработка лекционного материала. Самостоятельное изучение литературы. /Ср/	7	2	УК-4-З1 УК-4-З2 УК-4-У1	Л 1.2 Л 1.3 Л 2.2 Э 2 Э 3	
	Раздел 2. Социальная инженерия					
2.1	Социальная инженерия /Лек/	7	2	УК-4-З1 УК-4-З2	Э 2 Э 3	
2.2.	Использование утилит для сбора информации из открытых источников /Лр/	7	3	ОПК-4-У1 ОПК-4-В1 УК-4-У1	Л3.4	
2.3	Использование Social engineering toolkit в Kali Linux/Лр/	7	3	ОПК-4-У1 ОПК-4-В1 УК-4-У1	Л3.4	
2.4	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. /Ср/	7	2	УК-4-З1 УК-4-З2 УК-4-У1	Э 2 Э 3	
	Раздел 3. Понятия криптографии. Симметричные криптосистемы					

3.1	Понятия криптографии. Симметричные криптосистемы /Лек/	7	2	ПК-1-З2	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Э 3	
3.2	Шифрование данных методом замены в симметричных криптосистемах /Пр/	7	2	ПК-1-З2 ПК-1-В1	Л 3.2 Э 3	
3.3	Шифрование с использованием метода гаммирования и датчиков псевдослучайных чисел. Одноразовые блокноты /Пр/	7	2	ПК-1-З2 ПК-1-В1	Л 3.2 Э 3	
3.4	Использование утилит взлома паролей /Лр/	7	4	ОПК-4-У1 ОПК-4-В1	Л3.4	
3.5	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. Выполнение домашних заданий. /Ср/	7	3	ПК-1-З2 ПК-1-В1 ПК-1-У1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.2 Л 3.3 Э 3	
	Раздел 4. Асимметричные криптосистемы. Электронная цифровая подпись и хэш-функции. Криптоанализ					
4.1	Асимметричные криптосистемы /Лек/	7	2	ПК-1-З2 ПК-1-З1	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Э 1 Э 2 Э 3	
4.2	Электронная цифровая подпись и хэш-функции. Криптоанализ /Лек/	7	1	ПК-1-З1 ПК-1-З2	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Э 1 Э 2 Э 3	
4.3.	Шифрование данных в асимметричной криптосистеме RSA/Пр/	7	3	ПК-1-З2 ПК-1-В1 ПК-1-У1	Л 3.2 Э 3	
4.4	Алгоритм Диффи-Хелмана для безопасного обмена ключами/Пр/	7	3	ПК-1-З2 ПК-1-В1 ПК-1-У1	Л 3.2 Э 3	
4.5	Алгоритм электронной цифровой подписи RSA /Пр/	7	3	ПК-1-З2 ПК-1-В1 ПК-1-У1 ПК-1-В2 ПК-1-У2	Л 3.2 Э 3	
4.6	Алгоритм электронной цифровой подписи Эль-	7	4	ПК-1-З2 ПК-1-В1	Л 3.2 Э 3	

	Гамаля /Пр/			ПК-1-У1 ПК-1-В2 ПК-1-У2		
4.7.	Проработка лекционного материала. Самостоятельное изучение литературы. Подготовка к практическим занятиям. Выполнение домашнего задания /Ср/	7	3	ПК-1-З1 ПК-1-З2 ПК-1-В1 ПК-1-У1 ПК-1-У2	Л 1.1 Л 1.2 Л 1.3 Л 2.1 Л 2.2 Л 3.2 Э 1 Э 2 Э 3 Э 3	
	Раздел 5. Блокчейн и криптовалюта)					
5.1	Блокчейн и криптовалюта /Лек/	7	2	ПК-1-З1 ПК-1-З2	Э 2 Э 3	
5.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-З1 ПК-1-З2	Э 2 Э 3	
	Раздел 6. Идентификация и аутентификация	7				
6.1	Идентификация и аутентификация/Лек/	7	2	ПК-1-З1	Л 1.1 Э 1 Э 3	
6.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-З1	Л 1.1 Э 1 Э 3	
	Раздел 7. Веб-уязвимости					
7.1	Веб-уязвимости/Лек/	7	2	ПК-1-З3	Л 1.1 Э 1 Э 3	
7.2	SQL инъекции /Лр/	7	3	ПК-1-З3 УК-4-В1 ПК-1-В3	Л3.4	
7.3	Разновидности XSS атак/Лр/	7	4	ПК-1-З3 УК-4-В1 ПК-1-В3	Л3.4	
7.4	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	3	ПК-1-З3 УК-4-В1	Л 1.1 Э 1 Э 3	
	Раздел 8. Правовое регулирование					
8.1	Правовое регулирование /Лек/	7	2	ОПК-4-З1	Л 1.1 Л 1.2 Л 1.3 Э 1 Э 2 Э 3	
8.2	Проработка лекционного материала. Самостоятельное изучение литературы /Ср/	7	2	ОПК-4-З1	Л 1.1 Л 1.2 Л 1.3 Э 1 Э 2	

					Э 3	
	Часы на контроль /Контроль/	7	36	УК-4-З1 УК-4-З2 УК-4-У1 УК-4-В1 ОПК-4-З1 ОПК-4-У1 ОПК-4-В1 ПК-1-З1 ПК-1-З2 ПК-1-З3 ПК-1-У1 ПК-1-У2 ПК-1-В1 ПК-1-В2 ПК-1-В3	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 (*ПК-1-32)*
2. Абсолютно устойчивые криптосистемы по Шеннону и Керкгоффса (*ПК-1-32)*
3. Симметричные криптосистемы. Основные понятия (*ПК-1-32)*
4. Классификация симметричных криптоалгоритмов (*ПК-1-32)*
5. Шифр цезаря. Аффинный шифр (*ПК-1-32)*
6. Одноразовые блокноты. Гаммирование (*ПК-1-32)*
7. Блочные и поточные шифры. Основные понятия (*ПК-1-32)*
8. Сеть Фейстеля (*ПК-1-32)*
9. Алгоритм DES (*ПК-1-32)*
10. Алгоритм МАГМА (*ПК-1-32)*
11. Алгоритм Rijndael (*ПК-1-32)*
12. Алгоритм RC4 (*ПК-1-32)*

Раздел 4. Асимметричные криптосистемы. Электронная цифровая подпись и хэш-функции. Криптоанализ

1. Ассиметричные криптосистемы (*ПК-1-32)*
2. Односторонние функции (*ПК-1-32)*
3. Метод Эль-Гамаля (*ПК-1-32)*
4. Метод RSA (*ПК-1-32)*
5. Метод Диффи-Хелманна (*ПК-1-32)*
6. Хэш-функции. Свойства. (*ПК-1-32, ПК-1-31)*
7. ЭЦП. Свойства (*ПК-1-32, УК-4-33)*
8. «Хорошая» хэш-функция (*ПК-1-32, ПК-1-31)*
9. Основные понятия криптоанализа *(ПК-1-32)*
10. Частотный анализ, метод полного перебора и метод встречи по середине (парадокс дней рождений) *(ПК-1-32)*
11. Задачи факторизации и дискретного логарифмирования. *(ПК-1-32)*
12. «Радужные таблицы» *(ПК-1-32, ПК-1-31)*
13. «Соленый» хэш*(ПК-1-32, ПК-1-31)*

Раздел 5. Блокчейн и криптовалюта

1. Понятие блокчейна (*ПК-1-32, ПК-1-31)*
2. Пример работы биткоина (*ПК-1-32, ПК-1-31)*
3. Майнинг в сети биткоин (*ПК-1-32, ПК-1-31)*

4. Преимущества и недостатки блокчейн технологий. Сфера использования (*ПК-1-32, ПК-1-31)*

Раздел 6. Идентификация и аутентификация

1. СКУД-системы. (*ПК-1-31)*
2. Идентификация и аутентификация. (*ПК-1-31)*
3. Штрих-коды и QR-коды. (*ПК-1-31)*
4. RFID-метки. (*ПК-1-31)*
5. Биометрические способы идентификации. Недостатки. (*ПК-1-31)*
6. Виды аутентификации . (*ПК-1-31)*
7. Touch Memory. Карты доступа. (*ПК-1-31)*
8. Парольная аутентификация. . (*ПК-1-31)*
9. Ошибки при использовании паролей. Многофакторная аутентификация. . (*ПК-1-31)*
10. Одноразовые пароли. Повышения надежности парольной аутентификации. (*ПК-1-31)*
11. СМАРТ-карты. Электронные ключи. (*ПК-1-31)*

Раздел 7. Веб-уязвимости

1. Что такое инъекция (ПК-1-33)
2. XSS-атаки(ПК-1-33)
3. Предсказуемое расположение(ПК-1-33)
4. Классификация веб-угроз(ПК-1-33)

Раздел 8. Правовое регулирование информационной безопасности в РФ

1. Основные законы регулирующие защиту информации в РФ. (*ОПК-4-31)*
2. Роскомнадзор. ФСТЭК. Отдел «К» . (*ОПК-4-31)*

Перечень типовых задач для экзамена
(ПК-1-В1, ПК-1-В2)

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 предусмотрены 2 домашних задания:

1. Реализация алгоритма RC42. (ПК-1-32, ПК-1-В1, ПК-1-У1)
2. Частотный анализ во взломе шифров (ПК-1-32, ПК-1-В1, ПК-1-У1)

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 лэмьмг пмдцюьютъмпм дхищшчфпм, цмц дммкчшх, тцм фпм нмцёц эювфцо вэмф зищтюь. смпшъ ямгмдюхдё ъш смлшхю ю зъмпмльштюцфхоъм инзьхоъихдё. ксищоё лшпхмцюхю ъшщюэги. гшгмэм щф кьхм фпм ивюэхфьюф, гмпвш пмдцёзю мгшлшхюдо дмэдфз ъфльшгмзьф фзи хувю. эфсъфф, ъфльшгмзафз кьх цмхогм мвюъ. смпшъ ямтцю дсшли ильшх бцмпм эьдмгмпм пмдямвюъш. шсцис кфрхю, мыюафс шзфсюгшъдгмр сшлэфвгю, гмцмсьр вфэёцо хфц ъшлшв вмясшеюэшх смпшъш м цмз, тцм ясмюднмвюхм д ъюз э зуьнфъдгмз вэмсаф яснэмдивюё, ш ямцмз ясмдюх мямльшцо ямвмлсфэшфзьн э эмфъъьн ясфдцияхфъюён. кфрхю юлитшучфф ю нмхмвъм дзмцсфх ъш смпшъш, ямцмз ямгшлшх фзи дэмф ивмдцмэфсфьюф.

— цмхогм тцм юлитшх эшеф вмдоф, зюдцфс смпшъ, — дгшлшх кфрхю. — эь дмэдфз ъф ямнмцю ъш тфхмэфгш ъш цмр дцшсмр ымцмпсшыюю. зяфсэьф иэювфз дъмэш, ё ясмдцм эшд ъф ильшх.

— гмпвш бцм кьхм? — дясмдюх смпшъ.

— ъфвфху цмзи ъшлшв, ъш шэцмдфсэюдф и ксищофэ ысфрдхюъпмэ, — мцэфцюх кфрхю. цояютъьр ясфвдцшэюцфхо дсфвъфпм лшяшвш, дцмхо ншсшгцфсъьр ъфзъмпм пъидшэьр шзфсюгшъдгюр шгафъц, вш ю мвфщвш ю зшъфсш вфсщищодё цмщф цояютъм 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 юлитшщо эшеф хютъмф вфхм. ю циц эдяхьхм гмф-тцм фчф, ю ё лшцсфкмэшх зфдцьъф пшлфць, эьефвеюф лш эсфзё эшефпм ясфкьэшъюё э шэдцсюю ю пфсзшъюю. ю эдф дмехмдо. эшз ившхмдо эьдхфвюцо цфн дфзфсьн цюямэ юл зуьнфъш, ю эмц цфяфсо эь эфсъихюдо дувш, тцмкь ямикюэшцо юн эдфн. икюрдцэм змхоцгф э эфъф, лшцфз — гшсхш яышъш э пшзкиспф. ш дхфвиучюф э эшефз дяюдгф ксищоё ысфрдхюъпю, ё ъф меюкдё?

— ё ясюфншх дувш ясмвшэшцо гмзяоуцфсь, — идцшхм ю сшлвсшщфъъм мцэфцюх смпшъ. — бцм эдф.

кфрхю ямщшх яхфтшзю.

— зъф ъфэшщьм, тфз эь лвфдо лшъюзшфцфдо. ъф иямхъмзмтфъ дцмёцо ъш дцсшщф лшгмъмдцю э бцмр дцсшъф. ъм нмти ясфвиясфвюцо: сигю ясмто мц ысфрдхюъпмэ. ъф дзфрцф юн цсмпшцо. дхюегмз зъмпм эсфзфью ё ямцсшщюх 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 ямьёх, ямтфзи ксищоё ысфрдхюъпю кьхю цшг д ъюз хукфлъь ю всищфхукьь.

— 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 ясфвиясфщвшу: цмхогм ямясмкирцф ю дцшъфцф змюз эсшпмз.

смпшъ дзмцсфх ъш ъфпм нмхмвъм ю ясюдшхоъм.

— ъф ямъюзшу, м тфз бцм эь, ъм ямлэмхоцф ю зъф вщцо 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 ъфясюёцъмддцю. мвюъ, эдфпм мвюъ цфхфымъъьр лэмъмг, ю эь фф ъюгмпвш кмхоеф ъф иэювюцф

Перечень вопросов к домашнему заданию

(ПК-1-З2,ПК-1-З1, УК)

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

Так же предусмотрена курсовая работа на тему:

«Анализ угроз информационной безопасности и способы их решения» (ПК-1-З1, ПК-1-З3, УК-4-В1 , ПК-1-В3, ОПК-4-У1, ОПК-4-В1)

Содержание курсовой работы:

В курсовой работе необходимо проанализировать угрозы информационной безопасности и предложить решения по их минимизации

1. Проанализировать внутренние угрозы и предложить пути их устранения
2. Проанализировать внешние угрозы и пути их устранения
3. Нарисовать схему информационной безопасности

Перечень вопросов к защите курсовой работы

((ПК-1-З1, ПК-1-З3)

4. Чем отличаются внутренние и внешние угрозы
5. Как следует защищаться от внутренних угроз
6. Как защититься от НСД
7. Какие вы знаете современные сетевые экраны
8. Как защититься от различногорода инъекций
9. Как защититься от вирусов
10. Предложите способы резервирования данных
11. Где располагается ваша система
12. Правила хранения и формирования паролей
13. Защита от роботов

Также по дисциплине предусмотрено **5 лабораторных (ОПК-4-У1,ОПК-4-В1, ПК-1-З3,УК-4-В1 ,ПК-1-В3)**

и 6 практических работ (ПК-1-З2,ПК-1-В1,ПК-1-У1,,ПК-1-У2,ПК-1-В2), связанных с реализацией механизмов защиты в современных компьютерных системах

Перечень вопросов к защите лабораторных и практических работ

(ПК-1-З3, ПК-1-З2)

1. Что такое хэш-функция
2. Что такое симметричный криптоалгоритм?
3. Что такое асимметричный криптоалгоритм?
4. Какие вы знаете симметричные шифры?
5. Что такое открытый и закрытый ключ?

6. Что такое мод N?
7. Опишите, для чего используется расширенный алгоритм Евклида
8. Как хранятся пароли в различных операционных системах?
9. Чем отличается аффинный шифр от шифра Цезаря, что у них общего?
10. Что такое ЭЦП?
11. Чем отличается хэш-функция от ЭЦП?
12. Какие виды хэш-функций вы знаете?
13. Какие вы знаете ассиметричные шифры?
14. Можно ли взломать симметричный шифр путем перебора?
15. Можно ли взломать асимметричный шифр путем перебора?
16. Какие основные принципы разработки шифров?
17. Какие вы знаете виды сетевых атак?
18. Что такое фишинг?
19. Что такое DOS-атака?
20. ЭЦП. Свойства
21. Что такое идентификация и аутентификация?
22. Что такое односторонняя функция?
23. Доказано ли существование односторонних функций?
24. Что такое гаммирование?
25. Что такое ПСЧ-датчик?
26. Если докажут существование односторонних функций это хорошо или плохо для криптографии?
27. Если докажут что односторонних функций не существует,это хорошо или плохо для криптографии?
28. Виды аутентификации
29. В чем суть метода Эль-Гамаля
30. В чем суть метода RSA
31. В чем суть метода Диффи-Хелманна
32. Какие рекомендации по размеру ключей в асимметричных криптосистемах?
33. Классификация симметричных криптоалгоритмов
34. Что такое одноразовый блокнот

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»
09.03.02 Информационные системы и технологии
Профиль – – Информационные системы и технологии
Дисциплина «Информационная безопасность»

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;	«Неудовлетворительно»

			- незнание литературы, рекомендованной программой дисциплины.		
	3.	Курсовая работа	Компетенции сформированы. Курсовая работа выполнена в полном объеме; отчёт по работе оформлен в полном соответствии с предъявляемыми требованиями.	«Отлично»	
			Компетенции сформированы. Курсовая работа в целом выполнена правильно, расчеты содержат непринципиальные ошибки. Отчёт по работе оформлен в основном в соответствии с предъявляемыми требованиями	«Хорошо»	
			Компетенции сформированы. Курсовая работа в основной части выполнена; отчёт по работе оформлен с некоторыми отступлениями от предъявляемых требований.	«Удовлетворительно»	
			Компетенции не сформированы. Курсовая работа не выполнена, либо отчёт по работе отсутствует или его оформление не соответствует предъявляемым требованиям.	«Неудовлетворительно»	
	4	Устный опрос по материалам лабораторных и практических занятий	Обучающийся уверенно и правильно отвечает на вопросы	«Зачтено»	
			Обучающийся не верно отвечает на вопросы	«Не зачтено»	

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.	Системы защиты информации в ведущих зарубежных	ЭБС «Университетская библиотека онлайн» URL: http://biblioclub.ru/index.php?page=book&id=93351	М. : Флинта, 2016

	Кондрашин, М. В. Рудановский	странах: учебное пособие для вузов		
6.1.3. Методические разработки				
Обозначение	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л.3.1	Соловьев А.Ю.	Пособие по выполнение курсовой работы по курсу «Информационная безопасность»	**https://lms.misis.ru/enroll/RY9MET**	
Л 3.2	Соловьев А.Ю	Пособие к выполнению практических занятий по курсу «Информационная безопасность»	**https://lms.misis.ru/enroll/RY9MET**	
Л 3.3	Соловьев А.Ю	Пособие к выполнению домашних заданий по курсу «Информационная безопасность»	**https://lms.misis.ru/enroll/RY9MET**	
Л 3.4	Соловьев А.Ю	Лабораторный практикум по курсу «Информационная безопасность»	**https://lms.misis.ru/enroll/RY9MET**	
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			
П 3	Дистрибутив Kali Linux (свободно распространяемое программное обеспечение)			
П 4	Дистрибутив Ubuntu (свободно распространяемое программное обеспечение)			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ	
7.1	**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.
7.2	**Аудитория №404** **«Лаборатория объектно-ориентированного программирования»** Перечень основного оборудования, учебно-наглядных пособий: • персональный компьютер – 9 шт; • интерактивная доска;

	• проектор; • 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 и курсовой Обучение проводится в один семестр и организуется в соответствии с настоящей программой. Самостоятельная работа студентов осуществляется и контролируется с помощью: – индивидуального опроса студентов при защите лабораторных работ и практических занятий, – сдачи домашних заданий – защиты курсовой работы Экзамен проставляется при условии выполнения учебного плана дисциплины, и по результатам ответов на экзаменационные билеты