МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего образования
«Национальный исследовательский технологический университет «МИСИС»

Рабочая программа дисциплины (модуля)

Информационная безопасность

Закреплена за подразделением Кафедра инфокоммуникационных технологий

Направление подготовки 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА

Профиль

Квалификация **Бакалавр**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 51
самостоятельная работа 22
часов на контроль 35

Формы контроля в семестрах:
экзамен 4

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**4 (2.2)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	17	17	17	17
Лабораторные	17	17	17	17
Практические	17	17	17	17
Итого ауд.	51	51	51	51
Контактная работа	51	51	51	51
Сам. работа	22	22	22	22
Часы на контроль	35	35	35	35
Итого	108	108	108	108

Программу составил(и):

Старший преподаватель, Бахаров Леонид Ефимович

Рабочая программа

Информационная безопасность

Разработана в соответствии с ОС ВО:

Самостоятельно устанавливаемый образовательный стандарт высшего образования - бакалавриат Федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский технологический университет «МИСИС» по направлению подготовки 09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА (приказ от 02.04.2021 г. № 119 о.в.)

Составлена на основании учебного плана:

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА, 09.03.03-БПИ-23.plx , утвержденного Ученым советом НИТУ МИСИС в составе соответствующей ОПОП ВО 22.06.2023, протокол № 5-23

Утверждена в составе ОПОП ВО:

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА, , утвержденной Ученым советом НИТУ МИСИС 22.06.2023, протокол № 5-23

Рабочая программа одобрена на заседании

Кафедра инфокоммуникационных технологий

Протокол от 07.03.2023 г., №9

Руководитель подразделения Кузнецова Ксения Александровна

1. ЦЕЛИ ОСВОЕНИЯ	
1.1	Целями освоения дисциплины являются формирование у студентов знаний по основам инженерно-технической защиты информации, обеспечения конфиденциальности, целостности и доступности данных, а также навыков и умений в области анализа потенциальных угроз информационной безопасности, выборе средств реализации защиты в информационных системах.

2. МЕСТО В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ		
	Блок ОП:	Б1.О
2.1	**Требования к предварительной подготовке обучающегося:**	
2.1.1	Базы данных	
2.1.2	Объектно-ориентированное программирование	
2.1.3	Персональная эффективность	
2.1.4	Введение в специальность	
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**	
2.2.1	Подготовка к процедуре защиты и защита выпускной квалификационной работы	
2.2.2	Подготовка к процедуре защиты и защита выпускной квалификационной работы	

3. РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ФОРМИРУЕМЫМИ КОМПЕТЕНЦИЯМИ
УК-3: Способен эффективно обмениваться информацией, идеями, проблемами и решениями с инженерным сообществом и обществом в целом, осуществлять социальное взаимодействие и реализовывать свою роль в команде
Знать:
УК-3-З1 Основные типы вредоносных программ; методы защиты от компьютерных вирусов и других вредоносных программ; принципы сетевого экранирования; технологии построения обманных систем; основные технические каналы утечек информации; виды оборудования для защиты от утечек по техническим каналам.
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-3-З1 Основные понятия и определения в области информационной безопасности; источники, риски и формы атак на информационные системы; угрозы, которым подвергается информация; основные направления защиты информации; основные законодательные акты РФ в области информационной безопасности; ответственность за преступления в сфере компьютерной безопасности.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Знать:
УК-2-З1 Основные определения и принципы криптографии; наиболее распространенные симметричные и асимметричные криптографические алгоритмы; требования к криптографическим хэш-функциям; алгоритмы электронной цифровой подписи и атаки на них; сущность и алгоритм реализации протокола с нулевым разглашением; основные положения стеганографии; применение цифровых водяных знаков для защиты интеллектуальной собственности.
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
Уметь:
ОПК-3-У1 Выявлять источники, риски и формы атак на информацию; применять на практике международные и российские профессиональные стандарты информационной безопасности, современные парадигмы и методологии, инструментальные средства реализации информационной безопасности.
УК-3: Способен эффективно обмениваться информацией, идеями, проблемами и решениями с инженерным сообществом и обществом в целом, осуществлять социальное взаимодействие и реализовывать свою роль в команде
Уметь:
УК-3-У1 Сопоставлять различные виды вредоносного программного обеспечения и выбирать адекватные меры программно-аппаратной реализации средств защиты; определять возможные причины и пути утечек информации через сетевые экраны; рассчитывать расстояние до границы контролируемой зоны, требуемое для передачи конфиденциальной

информации по электромагнитному каналу; выбирать средства защиты информации, необходимые для предотвращения её утечек по техническим каналам.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Уметь:
УК-2-У1 Выбирать алгоритм криптографической защиты в соответствии с характером защищаемой информации; выполнять первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены; производить генерацию открытого и закрытого ключа и шифрование в алгоритмах RSA и ELGAMAL; находить хэш-образ заданного сообщения; проверять подлинность электронной цифровой подписи по схеме RSA.
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
Владеть:
ОПК-3-В1 Навыками определения критериев оценки безопасности сообщения, передаваемого по электромагнитному каналу; методикой организации защиты проводных линий от утечки информации; навыками работы с современными информационными системами и средствами обеспечения их информационной безопасности.
УК-2: Способен собирать и интерпретировать данные и определять круг задач в рамках поставленной цели, выбирать оптимальные способы решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений, умение обосновывать принятые решения
Владеть:
УК-2-В1 Владеть навыками шифрования информации, генерации открытых и закрытых ключей, вычисления значений хэш-функций и электронной цифровой подписи; навыками применения стеганографических методов и программ в задачах защиты информации.

4. СТРУКТУРА И СОДЕРЖАНИЕ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Формируемые индикаторы компетенций	Литература и эл. ресурсы	Примечание	КМ	Выполняемые работы
	Раздел 1. Организационная и правовая защита информации							
1.1	Лекция № 1. Введение в информационную безопасность. /Лек/	4	2	ОПК-3-З1	Л1.4 Л1.5Л2.14Л3.2 Л3.3 Э3			
1.2	Лекция № 2. Организационная и правовая защита информации. Выполнение контрольной работы 1. /Лек/	4	2	ОПК-3-З1	Л1.4 Л1.5Л2.14Л3.2 Л3.3 Э3			
1.3	Парольная защита информации. Выполнение практической работы 1. /Пр/	4	2	ОПК-3-У1	Л1.4Л2.14Л3.3 Э3			Р1
1.4	Исследование параметров парольной защиты. Оформление отчета по практической работе 1. /Ср/	4	1	ОПК-3-З1 ОПК-3-У1	Л1.4Л2.14Л3.3 Э3			
1.5	Изучение Доктрины информационной безопасности РФ и Закона о персональных данных. /Ср/	4	2	ОПК-3-З1	Л1.4Л2.14Л3.3 Э1 Э2 Э3		КМ1	
	Раздел 2. Криптографические методы защиты информации							

2.1	Лекция 3. Введение в криптографию /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			
2.2	Лекция 4. Симметричные криптографические алгоритмы. /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			
2.3	Лекция 5. Криптография с открытым ключом. /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			
2.4	Лекция 6. Криптографические хэш-функции. Электронная подпись. /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.10 Л2.12Л3.2 Л3.3 Л3.4 Э3			
2.5	Использование классических криптоалгоритмов подстановки для защиты текстовой информации. Выполнение раздела 1 лабораторной работы 1. /Лаб/	4	2	УК-2-У1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			
2.6	Использование классических криптоалгоритмов подстановки для защиты текстовой информации. Выполнение раздела 2 лабораторной работы 1. /Лаб/	4	2	УК-2-У1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			
2.7	Изучение операций в полях Галуа. Подготовка к выполнению лабораторной работы 2. /Лаб/	4	1	УК-2-З1 УК-2-У1	Л1.3 Л1.7Л2.4 Л2.8Л3.2 Л3.3 Л3.4 Э3			Р10
2.8	Стандарт симметричного шифрования AES RIJNDAEL. Выполнение лабораторной работы 2. /Лаб/	4	2	УК-2-З1 УК-2-У1	Л1.3 Л1.7Л2.4 Л2.8Л3.2 Л3.3 Л3.4 Э3			Р10
2.9	Блочные составные шифры. Выполнение раздела 1 лабораторной работы 3. /Лаб/	4	2	УК-2-У1	Л1.3 Л1.7Л2.2 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			Р11
2.10	Сеть Фейстеля. Выполнение раздела 2 лабораторной работы 3. /Лаб/	4	2	УК-2-У1	Л1.1 Л1.3 Л1.7Л2.2 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			Р11

2.11	Генерация простых чисел, используемых в асимметричных алгоритмах шифрования. Выполнение раздела 1 лабораторной работы 4. /Лаб/	4	2	УК-2-У1	Л1.3 Л1.7Л2.4 Л2.5 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			Р12
2.12	Сравнительное исследование теста пробных делений и теста Ферма. Выполнение раздела 2 лабораторной работы 4. /Лаб/	4	2	УК-2-У1	Л1.3 Л1.7Л2.4 Л2.5 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			Р12
2.13	Повышение криптостойкости шифров подстановки. Выполнение практической работы 2. /Пр/	4	2	УК-2-У1	Л1.3 Л1.7Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			Р2
2.14	Алгоритм симметричного шифрования ГОСТ 28147 – 89. Выполнение практической работы 3. /Пр/	4	2	УК-2-У1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			
2.15	Криптографические алгоритмы с открытым ключом. Выполнение практической работы 4. /Пр/	4	2	УК-2-В1	Л1.3 Л1.7Л2.11 Л2.12Л3.2 Л3.3 Л3.4 Э3			
2.16	Вычисление хэш-функций. Формирование и проверка электронной подписи. Выполнение практической работы 5. /Пр/	4	2	УК-2-У1	Л1.3 Л1.7Л2.10 Л2.12Л3.3 Л3.4 Э3			
2.17	Встраивание и извлечение цифровых водяных знаков. Алгоритм Лангелаара. Выполнение раздела 1 практической работы 6. /Пр/	4	2	УК-2-В1	Л1.4 Л1.5Л2.14Л3 .3 Л3.4 Э3			
2.18	Алгоритм Куттера. Выполнение раздела 2 практической работы 6. /Пр/	4	1	УК-2-В1	Л1.4 Л1.5Л2.14Л3 .3 Л3.4 Э3			Р6
2.19	Изучение особенностей простейших криптографических алгоритмов при защите текстовой информации. Оформление отчета по лабораторной работе 1. /Ср/	4	2	УК-2-З1 УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.5 Л2.6 Л2.7 Л2.10Л3.3 Л3.4 Э3			
2.20	Изучение шифров Плейфера, Хилла и Виженера. Оформление отчета по практической работе 2. /Ср/	4	2	УК-2-З1 УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3			

2.21	Изучение цикловых преобразований алгоритма AES. Оформление отчета по лабораторной работе 2. /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			
2.22	Исследование режима простой замены алгоритма ГОСТ 28147 – 89. Оформление отчета по практической работе 3. /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.5 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			
2.23	Исследование принципа работы сети Фейстеля. Оформление отчета по лабораторной работе 3. /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.5 Л2.8Л3.2 Л3.3 Л3.4 Э3			
2.24	Изучение алгоритмов шифрования RSA, KNAPSAK, EL GAMAL. Оформление отчета по практической работе 4. /Ср/	4	2	УК-2-З1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.7Л3.2 Л3.3 Л3.4 Э3			
2.25	Нахождение чисел Кармайкла в заданном интервале. Оформление отчета по лабораторной работе 4. /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.4 Л2.8Л3.2 Л3.3 Л3.4 Э3			
2.26	Изучение алгоритмов цифровой подписи RSA, EL GAMAL, DSA. Оформление отчета по практической работе 5. /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.6 Л2.7Л3.3 Л3.4 Э3			
2.27	Изучение алгоритмов встраивания и извлечения ЦВЗ. Оформление отчета по практической работе 6. /Ср/	4	1	УК-2-З1 УК-2-В1	Л1.4 Л1.5Л2.14Л3.3 Л3.4 Э3			
2.28	Выполнение контрольной работы 2. /Ср/	4	1	УК-2-З1 УК-2-У1 УК-2-В1	Л1.3 Л1.4 Л1.5 Л1.7Л2.2 Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3		КМ2	
	Раздел 3. Кибербезопасность							
3.1	Лекция 7. Вредоносное программное обеспечение. /Лек/	4	2	УК-3-З1	Л1.4 Л1.5Л2.9 Л2.13 Л2.14Л3.3 Э3			
3.2	Лекция 8. Программно-аппаратные средства обеспечения кибербезопасности. /Лек/	4	2	УК-3-З1	Л1.4Л2.9Л3.3 Э3			
3.3	Определение типа вредоносного программного обеспечения по заданному описанию. Выполнение практической работы 7. /Пр/	4	2	УК-3-У1	Л1.4 Л1.5 Л1.6Л2.9 Л2.13Л3.3 Э3			

3.4	Изучение классификации вредоносного программного обеспечения по методике Лаборатории Касперского. /Ср/	4	1	УК-3-З1	Л1.4 Л1.5Л2.14Л3.3 Э3			
3.5	Изучение правил поглощения и наименования вредоносного программного обеспечения. Оформление отчета по практической работе 7. /Ср/	4	1	УК-3-З1 УК-3-У1	Л1.4 Л1.5Л2.9 Л2.13 Л2.14Л3.3 Э3			
3.6	Изучение механизмов организации утечек через сетевой экран /Ср/	4	1	УК-3-У1	Л1.4 Л1.5Л2.3Л3.3 Э3			
3.7	Выполнение контрольной работы 3. /Ср/	4	1	УК-3-З1 УК-3-У1	Л1.4 Л1.5Л2.3Л3.3 Э3		КМ3	
	Раздел 4. Инженерно-техническая защита информации							
4.1	Лекция 9. Защита информации от утечек по техническим каналам. /Лек/	4	1	ОПК-3-З1	Л1.1 Л1.2Л2.1 Л2.9Л3.1 Л3.3 Э3			
4.2	Расчет радиуса безопасной зоны при передаче информации по электромагнитному каналу. Выполнение практической работы 8. /Пр/	4	2	ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			
4.3	Изучение фильтра "Гранит" для защиты слаботочных коммуникаций. выполнение лабораторной работы 5. /Лаб/	4	2	ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			
4.4	Расчет параметров электромагнитного канала утечки информации. Оформление отчета по практической работе 8. /Ср/	4	1	ОПК-3-У1 ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			
4.5	Изучение методов защиты проводных линий от утечки информации. Оформление отчета по лабораторной работе 5. /Ср/	4	1	ОПК-3-У1 ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

5.1. Контрольные мероприятия (контрольная работа, тест, коллоквиум, экзамен и т.п), вопросы для самостоятельной подготовки

Код КМ	Контрольное мероприятие	Проверяемые индикаторы компетенций	Вопросы для подготовки

КМ1	Контрольная работа № 1. Основные понятия и определения информационной безопасности	ОПК-3-З1;ОПК-3-У1	1. Основные свойства информации как объекта защиты, ее существенные признаки. 2. Основные факторы, способствующие повышению уязвимости информации 3. Классификация информации как объекта защиты 4. Угрозы, соответствие свойств и угроз информации 5. Основные параметры парольной защиты. Расчет длины пароля.
КМ2	Контрольная работа № 2. Криптография	УК-2-З1;УК-2-У1;УК-2-В1	1. Симметричные криптоалгоритмы: шифры Вернама, Цезаря, Виженера, Хилла, AES, ГОСТ-28147-89. 2. Сеть Фейстеля и ее свойства. 3. Алгоритмы с окрытым ключом: Диффи-Хэллмана, RSA, EL GAMAL, KNAPSAK 4. Алгоритмы хэширования 5. Алгоритмы электронной подписи: RSA, EL GAMAL, DSA. 6. Протокол доказательства с нулевым разглашением: алгоритм Фейга-Фиата-Шамира.
КМ3	Контрольная работа № 3. Вредоносное программное обеспечение	УК-3-З1;УК-3-У1	1. Классификация вредоносного ПО. Правила поглощения и наименования. 2. Принципы и механизмы антивирусной защиты 3. Сетевое экранирование. 4. Виды утечек 5. Обманные системы

КМ4	Экзамен	ОПК-3-З1;УК-3-З1;УК-3-У1;УК-2-З1;УК-2-У1;УК-2-В1;ОПК-3-В1;ОПК-3-У1	1. Принципы построения систем антивирусной защиты. 2. Задачи подразделения антивирусной защиты. 3. Состав современного антивирусного пакета. 4. Сигнатурный анализ при обнаружении вредоносных программ. Достоинства и недостатки. 5. Эвристический анализ при обнаружении вредоносных программ. Достоинства и недостатки. 6. Сетевые экраны. Определение, назначение, классификация. 7. Сетевые экраны. Утечки. Тесты на утечки. 8. Базовые идеи, позволяющие обойти защиту сетевого экрана. 9. Технологии организации утечек. Метод подмены файла доверенного процесса. 10. Технологии организации утечек. Запуск доверенного приложения с параметрами командной строки. 11. Технологии организации утечек. Внедрение динамической библиотеки в адресное пространство одного из доверенных процессов. 12. Технологии организации утечек. Внедрение кода в адресное пространство одного из доверенных процессов без использования динамической библиотеки. 13. Технологии организации утечек. Использование программных интерфейсов для управления браузером. 14. Технологии организации утечек. Использование программных интерфейсов, предоставляемых системными сервисами (System services). 15. Системы обнаружения атак. Назначение, классификация. 16. Механизм функционирования обманных систем при защите информации. 17. Обманные системы. Метод камуфляжа. 18. Обманные системы. Метод сокрытия. 19. Обманные системы. Метод дезинформации. 20. Аутентификация и идентификация. Определение. Методы аутентификации. 21. Парольные методы аутентификации. 22. Методы аутентификации, основанные на использовании уникального предмета. 23. Биометрические методы идентификации. 24. Разграничение доступа. Определение, основные методы. 25. Регистрация и аудит в системе защиты информации. 26. Акустический канал утечки информации. Принцип действия, методы защиты. 27. Виброакустический канал утечки информации. Принцип действия, методы защиты. 28. Электромагнитный канал утечки информации. Принцип действия, методы защиты. 29. Проводной канал утечки информации. Принцип действия, методы защиты. 30. Оптический канал утечки информации. Принцип действия, методы защиты. 31. Определение криптографии. Принципы Керкхофса. 32. Сервисы криптосистем. 33. Одноразовый шифровальный блокнот. Требования при использовании одноразовых блокнотов. 34. Шифры подстановки. Примеры реализации в симметричных криптоалгоритмах. 35. Шифры перестановки. Примеры реализации в симметричных криптоалгоритмах. 36. Симметичные и асимметричные криптоалгоритмы. Преимущества и недостатки. 37. Блочные и поточные шифры. Преимущества и недостатки. 38. Алгоритм Диффи-Хеллмана. Понятие о дискретном логарифмировании. Уязвимость к атаке «Человек посередине». 39. Алгоритм шифрования RSA. Создание открытого и секретного ключей. 40. Алгоритм Эль Гамаля. Работа в режиме шифрования.

			41. Криптосистемы с эллиптическими кривыми. 42. Последовательности Люка и их применение в криптографии. 43. Ранцевая криптосистема Меркля-Хеллмана. «Задача о рюкзаке» и ее применение в криптографии. 44. Доказательство с нулевым разглашением. Задача о «пещере Али Бабы». 45. Хэш-функции. Определение, классификация, требования к простейшим и криптографическим хэш-функциям. 46. Криптографическая стойкость хэш-функций. Коллизии первого и второго рода. Использование коллизий для взлома. 47. Алгоритмы криптостойкого хэширования. 48. Проблема аутентификации данных и электронная цифровая подпись. 49. Федеральный закон Российской Федерации от 6 апреля 2011 г. № 63-ФЗ "Об электронной подписи". Основные понятия и определения. 50. Алгоритм электронной цифровой подписи RSA и его недостатки. 51. Алгоритм электронной цифровой подписи Эль Гамаля. Его достоинства и недостатки. 52. Подделка электронной цифровой подписи. Классификация возможных результатов атак. Социальные атаки. 53. Управление ключами электронной цифровой подписи. Способы хранения закрытых ключей. 54. Компьютерная стеганография. Определение, основные понятия. 55. Применение стеганографии в системах защиты информации. Цифровые водяные знаки. 56. Встраивание цифровых водяных знаков. Алгоритм Лангелаара. 57. Встраивание цифровых водяных знаков. Алгоритм Куттера.

5.2. Перечень работ, выполняемых по дисциплине (Курсовая работа, Курсовой проект, РГР, Реферат, ЛР, ПР и т.п.)

Код работы	Название работы	Проверяемые индикаторы компетенций	Содержание работы
Р1	Практическая работа № 1. Расчет параметров парольной аутентификации	ОПК-3-З1	Изучить правила парольной защиты. Провести расчет и анализ основных параметров парольной аутентификации.
Р2	Практическая работа № 2. Повышение криптостойкости шифров подстановки	УК-2-З1;УК-2-У1;УК-2-В1	Изучение шифра Плейфера и многоалфавитного шифра Виженера.
Р3	Практическая работа № 3. Алгоритм симметричного шифрования ГОСТ 28147 – 89	УК-2-У1;УК-2-В1	Исследование работы алгоритма симметричного шифрования ГОСТ 28147 – 89 в режиме простой замены.
Р4	Практическая работа № 4. Криптографические алгоритмы с открытым ключом	УК-2-У1;УК-2-В1	Изучение работы алгоритмов шифрования RSA, Меркля-Хеллмана и Эль Гамаля

Р5	Практическая работа № 5. Вычисление хэш-функций. Формирование и проверка электронной подписи.	УК-2-У1;УК-2-В1	Изучение алгоритмов хэширования, постановки и проверки электронной подписи по схемам RSA, Эль Гамаля и DSA/
Р6	Практическая работа № 6. Стеганография	УК-2-З1;УК-2-В1	Изучение стеганографических алгоритмов Лангелаара и Куттера для встраивания цифровых водяных знаков в мультимедийный контент.
Р7	Практическая работа № 7. Классификация вредоносного программного обеспечения	УК-3-З1;УК-3-У1	Изучение классификации вредоносных программ, принятой в Лаборатории Касперского.
Р8	Практическая работа № 8. Методика определения критериев оценки безопасности сообщения, передаваемого по электромагнитному каналу	ОПК-3-В1	Ознакомление с требованиями стандартов электромагнитной совместимости (ЭМС) России, стран Европы и США. Изучение основных параметров электромагнитного канала утечки сообщений и методику определения критериев оценки безопасности сообщения, передаваемого по электромагнитному каналу(ЭМК). Исследование с помощью предложенной методики влияния различных видов ограждающих конструкций и уровня конфиденциальности передаваемых сообщений на параметры контролируемой зоны.
Р9	Лабораторная работа № 1. Использование классических алгоритмов подстановки и перестановки для защиты текстовой информации	УК-2-У1;УК-2-В1	1.Изучение простейших способов шифрования текстовой информации с помощью подстановки. 2. Изучение простейших способов шифрования текстовой информации с помощью перестановки.
Р10	Лабораторная работа № 2. Стандарт симметричного шифрования AES RIJNDAEL	УК-2-У1;УК-2-В1	Изучение стандарта симметричного шифрования AES RIJNDAEL
Р11	Лабораторная работа № 3. Изучение блочных составных шифров. Сеть Фейстеля	УК-2-У1;УК-2-В1	1. Изучение особенностей построения блочных криптографических алгоритмов 2. Изучение свойств архитектуры Фейстеля на примере кодирования и декодирования заданного сообщения.
Р12	Лабораторная работа № 4. Генерация простых чисел, используемых в асимметричных алгоритмах шифрования	УК-2-З1;УК-2-В1	1. Изучение критериев определения простых чисел и их применения в криптографии. 2. Сравнительное исследование теста пробных делений и теста Ферма.
Р13	Лабораторная работа № 5. Исследование фильтра Гранит для защиты проводных линий	ОПК-3-В1;ОПК-3-У1	Экспериментальное определение характеристик устройства защиты проводных линий от аппаратуры высокочастотного навязывания.

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

Экзаменационный билет состоит из двух теоретических вопросов и одной задачи. Задачи в билетах являются типовыми, подобные задачи обучающиеся решают в ходе выполнения практических и контрольных работ по данной дисциплине. Билеты хранятся на кафедре. Образец экзаменационного билета приведен в разделе Приложения.

Пример заданий экзаменационного билета:

1. Принципы построения систем антивирусной защиты.
2. Определение криптографии. Принципы Керкхофса.
3. Пусть пользователь А хочет передать пользователю В сообщение m=10, зашифрованное с помощью алгоритма RSA. Пользователь В имеет следующие параметры: P=7, Q=17, d=53. Вычислите значение С зашифрованного сообщения.

5.4. Методика оценки освоения дисциплины (модуля, практики. НИР)

Экзаменационная оценка:

Оценка "отлично" выставляется студенту, решившему задачу и полностью ответившему на два теоретических вопроса экзаменационного билета, обнаружившему всестороннее, систематическое и глубокое знание учебного материала, предусмотренного программой; усвоившему основную и знакомому с дополнительной литературой по программе; умеющему творчески и осознанно выполнять задания, предусмотренные программой; усвоившему взаимосвязь основных понятий и умеющему применять их к анализу и решению практических задач; безупречно выполнившему в процессе изучения дисциплины все задания, предусмотренные формами текущего контроля;

Оценки "хорошо" заслуживает студент, решивший задачу, ответивший полностью на один вопрос экзаменационного билета и не ответивший или ответивший частично на другой вопрос, при этом обнаруживший полное знание учебного материала, предусмотренного программой; успешно выполнивший все задания, предусмотренные формами текущего контроля;

Оценка "удовлетворительно" выставляется студенту, ответившему на два теоретических вопроса экзаменационного билета, но не решившего задачу, или решившего задачу, но не ответившего на два теоретических вопроса, или допустившему погрешности в ответе на экзамене или при выполнении экзаменационных заданий и обладающему необходимыми знаниями для их устранения под руководством преподавателя;

Оценка "неудовлетворительно" выставляется студенту, не ответившему на два вопроса экзаменационного билета и не решившему задачу, обнаружившему пробелы в знании основного материала, предусмотренного программой, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий; не выполнившему отдельные задания, предусмотренные формами текущего контроля.

Оценка за контрольные работы:

Контрольные работы состоят из 10 вопросов и проводятся в виде тестирования в LMS продолжительностью 15 минут (контрольная работа 1) или 45 минут (контрольные работы 2 и 3). За правильный ответ на каждый вопрос начисляется 0,5 балла. Максимальное количество баллов за одну работу равно 5.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.1	Иванов А. В., Трушин В. А.	Защита речевой информации от утечки по акустоэлектрическим каналам: учебное пособие	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2012
Л1.2	Голиков А. М.	Защита информации от утечки по техническим каналам: учебное пособие	Электронная библиотека	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015
Л1.3	Майстренко Н. В., Майстренко А. В.	Основы теории информации и криптографии: учебное электронное издание: учебное пособие	Электронная библиотека	Тамбов: Тамбовский государственный технический университет (ТГТУ), 2018

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л1.4	Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А.	Информационная безопасность и защита информации: учеб. пособие для студ. вузов, обуч. по спец. 230201 "Информационные системы и технологии"	Библиотека МИСиС	М.: ACADEMIA, 2008
Л1.5	Сергеев О. Н., Федоров Н. В.	Компьютерная защита информации: учеб. пособие для студ. спец. "Системы автоматизированного проектирования"	Библиотека МИСиС	М.: Изд-во МГГУ, 2007
Л1.6	Костин В. Н.	Методы и средства защиты компьютерной информации. Информационная безопасность компьютерных сетей (N 3085): учеб. пособие	Электронная библиотека	М.: [МИСиС], 2018
Л1.7	Костин В. Н.	Методы и средства защиты компьютерной информации. Криптографические методы защиты информации (N 3086): учеб. пособие	Электронная библиотека	М.: [МИСиС], 2018

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.1	Титов А. А.	Инженерно-техническая защита информации: учебное пособие	Электронная библиотека	Томск: Томский государственный университет систем управления и радиоэлектроники, 2010
Л2.2	Гультяева Т. А.	Основы теории информации и криптографии: курс лекций	Электронная библиотека	Новосибирск: Новосибирский государственный технический университет, 2010
Л2.3	Лапонина О. Р.	Межсетевое экранирование: учебное пособие	Электронная библиотека	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ) |Бином. Лаборатория знаний, 2007
Л2.4	Басалова Г. В.	Основы криптографии: курс лекций: курс лекций	Электронная библиотека	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2011
Л2.5	Лидовский В. В.	Основы теории информации и криптографии: курс: учебное пособие	Электронная библиотека	Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), 2007
Л2.6	Фороузан Б. А.	Математика криптографии и теория шифрования: учебное пособие	Электронная библиотека	Москва: Национальный Открытый Университет «ИНТУИТ», 2016
Л2.7	Лапонина О. Р.	Криптографические основы безопасности: учебное пособие	Электронная библиотека	Москва: Национальный Открытый Университет «ИНТУИТ», 2016
Л2.8		Криптографические методы защиты информации: лабораторный практикум: практикум	Электронная библиотека	Ставрополь: Северо-Кавказский Федеральный университет (СКФУ), 2015
Л2.9	Голиков А. М.	Защита информации в инфокоммуникационных системах и сетях: учебное пособие	Электронная библиотека	Томск: Томский государственный университет систем управления и радиоэлектроники, 2015

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л2.10	Ищукова Е. А., Лобова Е. А.	Криптографические протоколы и стандарты: учебное пособие	Электронная библиотека	Таганрог: Южный федеральный университет, 2016
Л2.11	Усенко О. А.	Приложения теории информации и криптографии в радиотехнических системах: учебное пособие	Электронная библиотека	Ростов-на-Дону, Таганрог: Южный федеральный университет, 2017
Л2.12	Кирпичников А. П., Хайбуллина З. М.	Криптографические методы защиты компьютерной информации: учебное пособие	Электронная библиотека	Казань: Казанский научно-исследовательский технологический университет (КНИТУ), 2016
Л2.13	Кубашева Е. С., Малашкевич И. А., Чекулаева Е. Н.	Информатика и вычислительная техника. Информационная безопасность автоматизированных систем: учебно-методическое пособие к прохождению производственной практики: учебно-методическое пособие	Электронная библиотека	Йошкар-Ола: Поволжский государственный технологический университет, 2019
Л2.14	Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф., Шаньгин В. Ф.	Защита информации в компьютерных системах и сетях	Библиотека МИСиС	М.: Радио и связь, 2001

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Библиотека	Издательство, год
Л3.1	Гуляев В. П.	Анализ демаскирующих признаков объектов информатизации и технических каналов утечки информации: учебно-методический комплекс	Электронная библиотека	Екатеринбург: Издательство Уральского университета, 2014
Л3.2	Ниссенбаум О. В.	Теоретико-числовые методы в криптографии. Сборник заданий: учебно-методическое пособие для студентов специальностей «Компьютерная безопасность» и «Информационная безопасность автоматизированных систем», направления «Информационная безопасность»: учебно-методическое пособие	Электронная библиотека	Тюмень: Тюменский государственный университет, 2014
Л3.3	Бахаров Л. Е.	Информационная безопасность и защита информации: сб. текстов	Библиотека МИСиС	М.: Изд-во МИСиС, 2015
Л3.4	Бахаров Л. Е.	Информационная безопасность и защита информации (разделы криптография и стеганография) (N 3854): практикум	Электронная библиотека	М.: [МИСиС], 2019

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

Э1	Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646).Режим доступа URL: http://kremlin.ru/acts/bank/41460 (дата обращения 22.02.2022).	http://kremlin.ru/acts/bank/41460

Э2	Федеральный Закон "О персональных данных" (с изменениями на 24 апреля 2020 года). Режим доступа URL: http://docs.cntd.ru/document/901990046 (дата обращения 22.02.2022).	http://docs.cntd.ru/document/901990046
Э3	Курс "Информационная безопасность" в ЭОИС Canvas. Режим доступа URL: https://lms.misis.ru/courses/3575 (дата обращения 22.02.2022).	https://lms.misis.ru/login/canvas

6.3 Перечень программного обеспечения

П.1	LMS Canvas
П.2	Microsoft Office
П.3	MATCAD

6.4. Перечень информационных справочных систем и профессиональных баз данных

И.1	1. Банк данных угроз безопасности информации (https://bdu.fstec.ru/)
И.2	2. Единое окно доступа к образовательным ресурсам (http://window.edu.ru)
И.3	3. Электронно-библиотечная система "Лань" (https://e.lanbook.com)
И.4	4. ScienceDirect - база полнотекстовых научных журналов и книг издательства Elsevier (https://www.sciencedirect.com)
И.5	5. Scopus - единая реферативная база данных научных публикаций (https://www.scopus.com)

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Ауд.	Назначение	Оснащение
Любой корпус Мультимедийная	Учебная аудитория для проведения занятий лекционного типа и/или для проведения практических занятий:	комплект учебной мебели до 36 мест для обучающихся, мультимедийное оборудование, магнитно-маркерная доска, рабочее место преподавателя, ПКс доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus
Л-728	Учебная аудитория	доска аудиторная меловая, экран проекционный, проектор, стационарные компьютеры 15 шт. ПО-Visual Studio; Electronic WorkBench; APACHE; MySQL; XAMPP; Python; комплект учебной мебели, пакет лицензионных программ MS Office
Л-731	Учебная аудитория	доска аудиторная меловая, экран проекционный, проектор, стационарные компьютеры 15 шт. ПО-Visual Studio; Electronic WorkBench; APACHE; MySQL; XAMPP; Python, комплект учебной мебели, пакет лицензионных программ MS Office
Читальный зал №3 (Б)		комплект учебной мебели на 44 места для обучающихся, МФУ Xerox VersaLink B7025 с функцией масштабирования текстов и изображений, 8 ПК с доступом к ИТС «Интернет», ЭИОС университета через личный кабинет на платформе LMS Canvas, лицензионные программы MS Office, MS Teams, ESET Antivirus.

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

Дисциплина относится к точным наукам и требует значительного объема самостоятельной работы. Отдельные учебные вопросы выносятся на самостоятельную проработку и контролируются посредством текущей аттестации. Качественное освоение дисциплины возможно только при систематической самостоятельной работе. Курсовое проектирование проводится с широким использованием компьютерных программ, как для выполнения, так и для оформления работы. Лабораторные работы выполняются с помощью компьютерных программ имитационного моделирования. Так как ситуация в сфере информационной безопасности непрерывно изменяется, кроме рекомендованной литературы, обучающимся следует активно использовать материалы периодической печати, сети интернет и социальных сетей, затрагивающие вопросы защиты информации. Приветствуется также посещение студентами специализированных выставок по направлению информационной безопасности и защиты информации с тем, чтобы сформировать наиболее целостное и актуальное представление об изучаемой дисциплине.

Занятия по дисциплине проводятся в компьютерных классах в ауд. Л-728, Л-731 (15 ПК в каждой) все компьютеры имеют выход в Интернет).