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

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-22.plx , утвержденного Ученым советом ФГАОУ ВО НИТУ "МИСиС" в составе соответствующей ОПОП ВО 22.09.2022, протокол № 8-22

Утверждена в составе ОПОП ВО:

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА, , утвержденной Ученым советом ФГАОУ ВО НИТУ "МИСиС" 22.09.2022, протокол № 8-22

Рабочая программа одобрена на заседании
Кафедра инфокоммуникационных технологий

Протокол от 07.06.2022 г., №9

Руководитель подразделения К.т.н., доц. Калашников Евгений Александрович

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	Введение в информационную безопасность. Организационная и правовая защита информации. /Лек/	4	2	ОПК-3-З1	Л1.4 Л1.5Л2.14Л3.2 Л3.3 Э3			
1.2	Парольная защита информации /Пр/	4	2	ОПК-3-У1	Л1.4Л2.14Л3.3 Э3		КМ1	Р1
1.3	Подготовка к защите практической работы /Ср/	4	1	ОПК-3-З1 ОПК-3-У1	Л1.4Л2.14Л3.3 Э3			
1.4	Самостоятельное изучение Доктрины информационной безопасности РФ и Закона о персональных данных. /Ср/	4	1	ОПК-3-З1	Л1.4Л2.14Л3.3 Э1 Э2 Э3		КМ1	
	Раздел 2. Математические методы защиты информации							
2.1	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		КМ2	

2.2	Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации /Лаб/	4	3	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			Р9
2.3	Подготовка к защите лабораторной работы /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			
2.4	Алгоритм симметричного шифрования ГОСТ 28147 – 89 /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			Р3
2.5	Подготовка к защите практической работы /Ср/	4	1	УК-2-З1 УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.5 Л2.6 Л2.7 Л2.10Л3.3 Л3.4 Э3			
2.6	Симметричные криптографические алгоритмы /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.10 Л2.11 Л2.12Л3.3 Л3.4 Э3		КМ2	
2.7	Повышение криптостойкости шифров подстановки /Пр/	4	2	УК-2-У1	Л1.3 Л1.7Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			
2.8	Подготовка к защите практической работы /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.5 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3		КМ10	
2.9	Блочные составные шифры. Сеть Фейстеля /Лаб/	4	4	УК-2-У1	Л1.3 Л1.7Л2.2 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			
2.10	Подготовка к защите лабораторной работы /Ср/	4	1	УК-2-У1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			

2.11	Асимметричная криптография /Лек/	4	2	УК-2-З1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5Л3.2 Л3.3 Л3.4 Э3			
2.12	Генерация простых чисел, используемых в асимметричных алгоритмах шифрования /Лаб/	4	4	УК-2-У1	Л1.3 Л1.7Л2.4 Л2.5 Л2.6 Л2.7Л3.2 Л3.3 Л3.4 Э3			
2.13	Подготовка к защите лабораторной работы /Ср/	4	1	УК-2-У1 УК-2 -В1	Л1.3 Л1.7Л2.2 Л2.5 Л2.8Л3.2 Л3.3 Л3.4 Э3		КМ7	
2.14	Криптографические алгоритмы с открытым ключом /Пр/	4	2	УК-2-В1	Л1.3 Л1.7Л2.11 Л2.12Л3.2 Л3.3 Л3.4 Э3			Р4
2.15	Подготовка к защите практической работы /Ср/	4	1	УК-2-З1 УК-2-В1	Л1.3 Л1.7Л2.2 Л2.4 Л2.5 Л2.7Л3.2 Л3.3 Л3.4 Э3		КМ12	
2.16	Стандарт симметричного шифрования AES RIJNDAEL /Лаб/	4	4	УК-2-З1 УК-2-У1	Л1.3 Л1.7Л2.4 Л2.8Л3.2 Л3.3 Л3.4 Э3			
2.17	Подготовка к защите лабораторной работы /Ср/	4	1	УК-2-У1 УК-2 -В1	Л1.3 Л1.7Л2.4 Л2.8Л3.2 Л3.3 Л3.4 Э3		КМ5	
2.18	Криптографические хэш-функции. Электронная подпись. /Лек/	4	3	УК-2-З1	Л1.3 Л1.7Л2.10 Л2.12Л3.2 Л3.3 Л3.4 Э3			
2.19	Вычисление хэш-функций. Формирование и проверка ЭЦП /Пр/	4	2	УК-2-У1	Л1.3 Л1.7Л2.10 Л2.12Л3.3 Л3.4 Э3			Р5
2.20	Подготовка к защите практической работы /Ср/	4	1	УК-2-У1 УК-2 -В1	Л1.3 Л1.7Л2.6 Л2.7Л3.3 Л3.4 Э3		КМ13	
2.21	Встраивание и извлечение цифровых водяных знаков. Алгоритм Лангелаара. Алгоритм Куттера /Пр/	4	3	УК-2-В1	Л1.4 Л1.5Л2.14Л3 .3 Л3.4 Э3			Р6
2.22	Подготовка к защите практической работы /Ср/	4	1	УК-2-З1 УК-2-В1	Л1.4 Л1.5Л2.14Л3 .3 Л3.4 Э3		КМ14	
	Раздел 3. Кибербезопасность							

3.1	Обзор вредоносного программного обеспечения /Лек/	4	2	УК-3-З1	Л1.4 Л1.5Л2.9 Л2.13 Л2.14Л3.3 Э3			
3.2	Самостоятельное изучение классификации вредоносного программного обеспечения по методике Лаборатории Касперского /Ср/	4	2	УК-3-З1	Л1.4 Л1.5Л2.14Л3 .3 Э3			
3.3	Определение типа вредоносного программного обеспечения по заданному описанию /Пр/	4	2	УК-3-У1	Л1.4 Л1.5 Л1.6Л2.9 Л2.13Л3.3 Э3		КМ3	Р7
3.4	Подготовка к защите практической работы /Ср/	4	2	УК-3-З1 УК-3-У1	Л1.4 Л1.5Л2.9 Л2.13 Л2.14Л3.3 Э3			
3.5	Программно-аппаратные средства обеспечения кибербезопасности /Лек/	4	2	УК-3-З1	Л1.4Л2.9Л3. 3 Э3			
3.6	Изучение механизмов организации утечек через сетевой экран /Ср/	4	2	УК-3-У1	Л1.4 Л1.5Л2.3Л3. 3 Э3			
	Раздел 4. Инженерно-техническая защита информации							
4.1	Защита информации от утечек по техническим каналам /Лек/	4	2	ОПК-3-З1	Л1.1 Л1.2Л2.1 Л2.9Л3.1 Л3.3 Э3			
4.2	Изучение методики расчета радиуса безопасной зоны при передаче информации по электромагнитному каналу /Пр/	4	2	ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			Р8
4.3	Подготовка к защите практической работы /Ср/	4	2	ОПК-3-У1 ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			
4.4	Изучение фильтра "Гранит" для защиты слаботочных коммуникаций /Лаб/	4	2	ОПК-3-В1	Л1.1 Л1.2Л2.1 Л2.9Л3.3 Э3			Р13
4.5	Подготовка к защите лабораторной работы /Ср/	4	2	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	ОПК-3-З1;ОПК-3-У1	1. Существенными признаками понятия «информационная безопасность» являются (выберите несколько ответов): - конфиденциальность - секретность

	информационной безопасности		- устойчивость к взлому - целостность - надёжность - доступность 2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления – это (выберите один правильный ответ): - документированная информация - информация - конфиденциальная информация - документ 3. К информационным процессам относятся (выберите несколько ответов): - создание информации - защита информации - сбор информации - обработка информации - накопление информации - поиск информации 4. Свойство информации, значение которого устанавливается владельцем информации и отражает ограничение доступа к ней - это (выберите один правильный ответ): - конфиденциальность - целостность - доступность - достоверность 5. По конечному проявлению различают следующие угрозы информации (выберите несколько ответов): - Блокирование - Ознакомление - Структурирование - Взлом - Модификация - Уничтожение 6. Модификация информации направлена на изменение таких свойств как (выберите несколько ответов): - Конфиденциальность - Доступность - Достоверность - Надёжность - Устойчивость - Целостность 7. Уничтожение информации направлено на (выберите несколько ответов): - Конфиденциальность - Доступность - Достоверность - Надёжность - Устойчивость - - Целостность 8. Неправомерное овладение конфиденциальной информацией возможно за счет (выберите несколько ответов): - разглашения - блокирования - несанкционированного доступа - утечки 9. Определить мощность пространства паролей, обеспечивающую требуемый уровень надежности парольной защиты (вероятность вскрытия 10-4) в течение 48 часов, если противник может реализовать скорость интерактивного подбора паролей 5

			паролей/мин. 10. Рассчитать минимальный срок действия пароля, при котором обеспечивается требуемый уровень надежности парольной защиты. Исходные данные: Вероятность вскрытия 10^-5. Мощность алфавита – 10 знаков. Длина пароля – 5 знаков. Скорость интерактивного подбора паролей - 10 паролей/минуту.
КМ2	Контрольная работа № 2. Криптография	УК-2-З1;УК-2-У1;УК-2-В1	1. Какой алгоритм применяется для реализации протокола идентификации с нулевым разглашением: A. алгоритм Диффи-Хеллмана B. алгоритм Эль-Гамаля C. алгоритм Меркля D. алгоритм Фейга-Фиата-Шамира 2. Какой алгоритм не является алгоритмом с открытым ключом: A. алгоритм RSA B. алгоритм Эль-Гамаля C. алгоритм DES D. алгоритм LUC 3. Какой алгоритм не является алгоритмом криптографического хэширования: A. алгоритм MD5 B. алгоритм CRC 32 C. алгоритм SHA D. алгоритм ГОСТ 34.11-94 4. Какой алгоритм не применяется для электронной цифровой подписи: A. алгоритм Диффи-Хеллмана B. алгоритм Эль-Гамаля C. алгоритм Меркля-Хеллмана D. алгоритм Фейга-Фиата-Шамира 5. Какой алгоритм не является алгоритмом с секретным ключом: A. алгоритм DES B. алгоритм IDEA C. алгоритм DSA D. алгоритм AES 6. Вычислить 7^-1 mod 10 7. Для указанного открытого ключа n=55, e=3 пользователя RSA проверить подлинность подписанного сообщения: <7,28>. Если подпись верна, в ответе записать 1, иначе – 0. 8. Пусть общие параметры для некоторого сообщества пользователей при использовании алгоритма Эль Гамаля p=23 и g=5, секретный ключ x=7. Вычислить открытый ключ y. 9. Заданы параметры p = 19 и q = 6 для протокола Диффи-Хеллмана и закрытые ключи пользователей a = 12 и b = 13. Найти общий секретный ключ. 10. Зашифруйте сообщение m шифром Вернама с ключом k: m = 1010101010, k = 0111001011.

КМ3	Контрольная работа № 3. Вредоносное программное обеспечение	УК-3-З1;УК-3-У1	1. Выберите верные высказывания: а) вирусом называется только такой код, который создан специально для дальнейшего самостоятельного распространения б) заражая файл, вирус записывает свой код только в начало файла в) макровирус записывает свой код в главную загрузочную запись Master Boot Record диска г) заражение почтовым вирусом происходит только в результате действий пользователей 2. Что такое бестелесный вирус? 3. По какому критерию определяется принадлежность вирусов к категории известных? 4. По предложенному описанию определите тип вредоносной программы: Содержит три макроса: AutoOpen, RepToDocs, RepToNormal. При открытии зараженного документа создает в корневом каталоге диска C: временный файл Tmp.bas, в который записывает свой код, после чего импортирует его в normal.dot, таким образом получая возможность для заражения других открываемых документов в MS Word. После заражения текущего документа удаляет с диска Tmp.bas. Не содержит никаких деструктивных функций. 5. По предложенному описанию определите тип вредоносной программы: Распространяется через интернет в виде файлов, прикрепленных к зараженным письмам. Является приложением Windows (PE EXE-файл), имеет размер около 6K (упакован UPX, размер распакованного файла - около 15K), написан на Visual Basic. Активизируется, только если пользователь сам запускает зараженный файл (при двойном щелчке на вложении). Реальное .EXE-имя файла во вложении скрыто "ложным" .JPG-именем при помощи дополнительных возможностей MS Outlook. Таким образом, зараженное EXE-вложение в письме выглядит как .JPG-файл, однако при открытии этого вложения оно обрабатывается как EXE-файл. Вложения подобного рода автоматически блокируются по умолчанию версиями MS Outlook 97 SP2 и выше.Затем инсталлирует себя в систему и запускает процедуры своего распространения. 6. По предложенному описанию определите тип вредоносной программы: Программа написана на Visual Basic, упакована PESpin. Размер файла - около 270 КБ.Распространяется при помощи Windows Messenger, рассылая по контакт-листу ссылку на зараженный файл. Устанавливает в систему Backdoor.Win32.Rbot. Может копировать себя в файлы webcam.pif, hot.pif, rofl.pif и др. в корень диска C:. 7. По предложенному описанию определите тип вредоносной программы: Программа написана на Visual Basic, ничем не упакована. Состоит из двух компонентов: клиентской (размер файла — 24576 байт) и серверной (размер — 16384 байт). Серверная компонента скрытно открывает порт 4567 и ждет соединения с клиентом. Клиентская компонента отображает окно с надписью «File Nail» и позволяет подключиться к серверу на заданном IP. 8. По предложенному описанию определите тип вредоносной программы: Выполнена в виде драйвера ядра NT (kernel mode driver).Файл программы имеет размер 5760 байт и часто называется msdirect.sys. При загрузке перехватывает системные сервисы путем замены обработчика в KeServiceDescriptorTable: • ZwQueryDirectoryFile, для сокрытия наличия файлов на диске; • ZwQuerySystemInformation, для сокрытия процессов; • ZwOpenFile, для блокирования доступа к своим файлам (не реализовано); • ZwQueryValueKey, для сокрытия занчений ключей реестра (не реализовано). Под Windows XP и выше, вероятнее всего, будет инициировать системный сбой (BSOD). Никаких других действий не производит. 9. По предложенному описанию определите тип вредоносной программы:

			При инсталляции копирует себя в системный каталог Windows под именем "rundll32.exe" и регистрируется в ключе автозапуска системного реестра: [HKLM\Software\Microsoft\Windows\CurrentVersion\Run\ControlPanel] Заменяет в системном каталоге Windows файл "msblank.htm". В изменённом "msblank.htm" содержится ссылка на сайт "cploving.awmhost.net", в результате чего пользователь вместо пустой страницы в Internet Explorer будет каждый раз заходить на этот сайт. 10. По предложенному описанию определите тип вредоносной программы: Программа позволяет производить сканирование IP-адресов в указанном пользователем диапазоне и предоставляет следующую информацию о компьютерах: • имя рабочей группы; • установленную операционную систему и ее версию; • время отклика; • MAC-адрес; • доступные ресурсы; Также программа имеет функцию подбора паролей.
КМ4	Защита лабораторной работы № 1.	УК-2-З1;УК-2-У1;УК-2-В1	Какие Вы знаете методы криптографической защиты файлов? В чем преимущества и недостатки одноалфавитных методов? Если Вам необходимо зашифровать текст, содержащий важную информацию, какой из рассмотренных в работе методов Вы выберете? Обоснуйте свой выбор. Целесообразно ли повторно применять для уже зашифрованного текста шифр Цезаря? Целесообразно ли повторно применять для уже зашифрованного текста метод многоалфавитного шифрования?
КМ5	Защита лабораторной работы № 2.	УК-2-З1;УК-2-У1;УК-2-В1	Сравнить основные характеристики алгоритмов Rijndael и ГОСТ 28147—89. Сравнить основные характеристики алгоритмов Rijndael и DES. Описать структуру сети Фейстеля. Привести обобщенные схемы шифрования данных с помощью алгоритма Rijndael и ГОСТ 28147—89. Дать их сравнительный анализ. Сравнить один раунд шифрования данных с помощью алгоритма Rijndael и ГОСТ 28147—89. Сравнить эквивалентность прямого и обратного преобразований в алгоритмах Rijndael и ГОСТ 28147—89. Сравнить выработку ключевой информации в алгоритмах Rijndael и ГОСТ 28147—89. Сравнить алгоримы Rijndael и ГОСТ 28147—89 по показателям диффузии. Сравнить алгоримы Rijndael и ГОСТ 28147—89 по показателям стойкости. Сравнить алгоримы Rijndael и ГОСТ 28147—89 по показателям производительности и удобству реализации.
КМ6	Защита лабораторной работы № 3.	УК-2-З1;УК-2-У1;УК-2-В1	Поясните принцип работы сети Фейстеля. В каких современных симметричных системах шифрования используется сеть Фейстеля? В чем отличие сбалансированной сети Фейстеля от несбалансированной сети Фейстеля? В каких блочных криптосистемах используется сбалансированная сеть? В каких современных симметричных системах шифрования не используется сеть Фейстеля? Какие механизмы шифрования используются в этих криптографических системах? Какой длины используются блоки для шифрования и цикловые ключи в блочных криптосистемах DES, FIAL, Blowfish,ГОСТ-28147—89? Какова надежность алгоритмов, использующих сеть Фейстеля? От чего она зависит?

КМ7	Защита лабораторной работы № 4.	УК-2-У1;УК-2-В1	Что такое тест Ферма на простоту и на каких математических фактах он основан? Что такое решето Эратосфена? Почему в качестве первого основания в тестах типа теста Ферма для проверки на простоту очень больших чисел целесообразно использовать число 2? Какова вероятность P(x) того, что наугад взятое нечетное очень большое число, не превосходящее x, окажется простым? Вычислить: 1711 (mod 13), 129 (mod 7). Сформулируйте суть теста на простоту с использованием пробных делений. Что такое числа Кармайкла?
КМ8	Защита лабораторной работы № 5.	УК-3-З1;УК-3-У1	Какие устройства могут быть использованы в качестве индукционного микрофона? Приведите примеры. Что такое АКУИ? Классификация методов использования электрической линии в качестве канала утечки информации. Поясните метод высокочастотного навязывания. Поясните метод синфазного маскирующего низкочастотного сигнала. Поясните метод высокочастотной маскирующей помехи. Поясните метод ультразвуковой маскирующей помехи. Поясните метод повышения напряжения. Поясните метод обнуления. Поясните компенсационный метод. Поясните метод выжигания. Что такое скремблирование сигнала и как оно применяется при защите проводных коммуникаций? Поясните использование фильтров для защиты проводных коммуникаций.
КМ9	Защита практической работы № 1	ОПК-3-З1;ОПК-3-У1	Какие правила парольной защиты Вам известны? Каким образом можно задать сложный для подбора, но легко запоминающийся пароль? От каких факторов зависит минимальная длина пароля? Каких паролей следует избегать? Что нужно сделать при компроментации пароля? Известно, что вероятность подбора пароля в течение его срока действия равна P=10^-6. Скорость интерактивного подбора паролей V = 10 паролей/мин. Время действия пароля одна неделя. Необходимо найти минимальную длину пароля, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль. Определить мощность пространства паролей, обеспечивающую требуемый уровень надежности парольной защиты (вероятность вскрытия 10^-4) в течении 48 часов, если противник может реализовать скорость интерактивного подбора паролей 5 паролей/мин. Рассчитать минимальный срок действия пароля, при котором обеспечивается требуемый уровень надежности парольной защиты. Вероятность вскрытия 10^-5, мощность алфавита – 10 знаков, длина пароля – 5 знаков. Скорость интерактивного подбора паролей - 10 паролей/минуту. Найти минимальную длину пароля, для алфавита мощностью 26 знаков, которая обеспечит его стойкость в течение одного дня непрерывных попыток подобрать пароль. При условии, что скорость интерактивного подбора паролей 10 паролей/мин, и вероятность подбора пароля в течение его срока действия равна 10^-4.

КМ10	Защита практической работы № 2	УК-2-З1;УК-2-У1;УК-2-В1	Какие подходы применяются в криптографии для повышения криптостойкости шифров подстановки? Поясните методику шифрования информации с помощью шифра Плейфера. Поясните методику дешифрования информации с помощью шифра Плейфера. Что является ключом в шифре Плейфера? К какому типу шифров относится шифр Плейфера? В чем заключаются преимущества и недостатки этой группы шифров? Поясните методику шифрования информации с помощью шифра Хилла. Поясните методику дешифрования информации с помощью шифра Хилла. Что является ключом в шифре Хилла? К какому типу шифров относится шифр Хилла? В чем заключаются преимущества и недостатки этой группы шифров? Поясните методику шифрования информации с помощью шифра Виженера. Поясните методику дешифрования информации с помощью шифра Виженера. Что является ключом в шифре Виженера? К какому типу шифров относится шифр Виженера? В чем заключаются преимущества и недостатки этой группы шифров?
КМ11	Защита практической работы № 3	УК-2-У1;УК-2-В1	К какому классу криптографических алгоритмов относится алгоритм шифрования ГОСТ 28147 – 89 ? Какие режимы работы алгоритма шифрования ГОСТ 28147 – 89 Вы знаете ? Каково их назначение ? Каким образом работает блок подстановки в алгоритме шифрования ГОСТ 28147 – 89 ? Какие размеры блока и ключа использует алгоритм шифрования ГОСТ 28147 – 89 ? Что такое имитовставка? Какой алгоритм пришел на смену алгоритму шифрования ГОСТ 28147 – 89 ? Что такое гаммирование и каким образом оно используется в алгоритме шифрования ГОСТ 28147 – 89 ? Каким образом в алгоритме шифрования ГОСТ 28147 – 89 достигается повышение криптостойкости ?
КМ12	Защита практической работы № 4	УК-2-В1;УК-2-У1	Какие криптографические алгоритмы с открытым ключом Вам известны? В чём заключается суть шифрования с открытым ключом? На каких типах односторонних преобразований основаны алгоритмы с открытым ключом? Поясните, каким образом производится генерация ключей в алгоритме RSA. Поясните, каким образом производится шифрование информации в алгоритме шифрования RSA. Поясните, каким образом производится дешифрование информации в алгоритме шифрования RSA. Поясните, каким образом производится генерация ключей в алгоритме шифрования на основе задачи об укладке ранца. Поясните, каким образом производится шифрование информации в алгоритме шифрования на основе задачи об укладке ранца. Поясните, каким образом производится дешифрование информации в алгоритме шифрования на основе задачи об укладке ранца. Поясните, каким образом производится генерация ключей в алгоритме шифрования Эль-Гамаля. Поясните, каким образом производится шифрование информации в алгоритме шифрования Эль-Гамаля. Поясните, каким образом производится дешифрование информации в алгоритме шифрования Эль-Гамаля.

КМ13	Защита практической работы № 5	УК-2-У1;УК-2-В1	Что такое хэш-функция? Какие требования предъявляются к криптографическим хэш-функциям? Что такое коллизии? От чего зависит криптографическая стойкость хэш-функций? Какие алгоритмы хэширования Вам известны? Что такое цифровая подпись? Какими свойствами она должна обладать? Какие алгоритмы постановки и проверки цифровой подписи Вы знаете? Поясните, каким образом производится генерация ключей в алгоритме цифровой подписи RSA. Поясните, каким образом производится постановка подписи в алгоритме цифровой подписи RSA. Поясните, каким образом производится проверка подписи в алгоритме цифровой подписи RSA. Поясните, каким образом производится генерация ключей в алгоритме цифровой подписи Эль-Гамаля. Поясните, каким образом производится постановка подписи в алгоритме цифровой подписи Эль-Гамаля. Поясните, каким образом производится проверка подписи в алгоритме цифровой подписи Эль-Гамаля. Поясните, каким образом производится генерация ключей в алгоритме цифровой подписи DSA. Поясните, каким образом производится постановка подписи в алгоритме цифровой подписи DSA. Поясните, каким образом производится проверка подписи в алгоритме цифровой подписи DSA.
КМ14	Защита практической работы № 6	УК-2-З1;УК-2-В1	Что такое стеганография и чем она отличается от криптографии? Что такое стегосистема? Какие требования предъявляются к стегосистемам? Какие методы защиты авторских прав на цифровой контент Вы знаете? Что такое цифровые водяные знаки и для чего они используются? Какие алгоритмы встраивания цифровых водяных знаков Вам известны? В чем состоит суть метода LSB ? Каковы его достоинства и недостатки? Что такое робастость цифрового водяного знака? Каким образом производится встраивание одного бита цифрового водяного знака в алгоритме Лангелаара? Каким образом производится извлечение одного бита цифрового водяного знака в алгоритме Лангелаара? Каким образом производится встраивание одного бита цифрового водяного знака в алгоритме Куттера? Каким образом производится извлечение одного бита цифрового водяного знака в алгоритме Куттера? Почему в алгоритме Куттера производится встраивание в канал синего цвета?

КМ15	Защита практической работы № 7	УК-3-З1;УК-3-У1	Поясните состав дерева детектируемых объектов. Какими современными вредоносными программами Вы бы его дополнили? Чем вирусы и черви отличаются от других вредоносных программ? Какие разновидности вирусов Вы знаете? Что такое троянские программы? По какому признаку их можно отличить от других вредоносных программ? Что такое эксплойты и для чего они используются злоумышленниками? Почему руткит относится к вредоносному программному обеспечению? Каким путем на компьютер пользователя попадают программы типа Adware? Что это за программы и чем они детектируются? Как различаются детектируемые объекты по типу совершаемых ими действий? Перечислите основные типы червей и охарактеризуйте их особенности их особенности. Какие методы используют черви для поиска адресов электронной почты? Чем вирусы отличаются от червей? Приведите примеры. Какие типы троянских программ Вы знаете? Назовите их особенности. Охарактеризуйте потенциально нежелательные программы. Приведите примеры. Для чего применяются правила поглощения типов детектируемых объектов? В чем заключаются эти правила?
КМ16	Защита практической работы № 8	ОПК-3-У1;ОПК-3-В1;ОПК-3-З1	При каких условиях возможна утечка информации по электромагнитному каналу? Какие помехи называются аддитивными? Приведите примеры. Что служит количественной мерой атмосферных помех при оценке электромагнитного канала утечки информации? При каких условиях невозможно понимание смысла перехваченного сообщения и скрытие признака наличия сообщения? Назовите известные Вам способы защиты информации от утечки по электромагнитному каналу. Какая ширина полосы пропускания разведывательного приемника обычно используется при расчетах? Что является критерием безопасной передачи информации по электромагнитному каналу? От каких параметров зависит и каким образом вычисляется напряженность поля атмосферных шумов? Из чего состоит канал утечки информации по электромагнитному каналу? Как зависит радиус защитной зоны от характера передаваемой информации? Как зависит радиус защитной зоны от рельефа местности и плотности застройки? Как зависит радиус защитной зоны от толщины и материала стен здания? Как зависит радиус защитной зоны от температуры окружающего воздуха?

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. Криптографически е 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	Изучение простейших способов шифрования текстовой информации и методов их криптоанализа.
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	Изучение особенностей построения блочных криптографических алгоритмов и свойств архитектуры Фейстеля
Р12	Лабораторная работа № 4. Генерация простых чисел, используемых в асимметричных алгоритмах шифрования	УК-2-З1;УК-2-В1	Изучение критериев определения простых чисел и их применения в криптографии.

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.

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

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).