

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Косенок Сергей Михайлович
Должность: ректор
Дата подписания: 18.06.2024 18:21:29
Уникальный программный ключ:
e3a68f3eaa1e62674b54f4998099d3d6bfdcf836

Бюджетное учреждение высшего образования
Ханты-Мансийского автономного округа-Югры
"Сургутский государственный университет"

УТВЕРЖДАЮ
Проректор по УМР

_____ Е.В. Коновалова

16 июня 2022 г., протокол УС №6

МОДУЛЬ ОБЩЕПРОФЕССИОНАЛЬНЫХ ДИСЦИПЛИН

Защита информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой	Автоматизированных систем обработки информации и управления		
Учебный план	b090301-АСОИУ-22-4.plx 09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА Направленность (профиль): Автоматизированные системы обработки информации и управления		
Квалификация	бакалавр		
Форма обучения	очная		
Общая трудоемкость	2 ЗЕТ		
Часов по учебному плану	72	Виды контроля в семестрах:	
в том числе:		зачеты 8	
аудиторные занятия	36		
самостоятельная работа	36		

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	8 (4.2)		Итого	
	уп	рп		
Неделя	10 1/6			
Вид занятий	уп	рп	уп	рп
Лекции	24	24	24	24
Лабораторные	12	12	12	12
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	36	36	36	36
Итого	72	72	72	72

Программу составил(и):

к.т.н., Доцент, Гавриленко Т.В.

Рабочая программа дисциплины

Защита информации

разработана в соответствии с ФГОС:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 09.03.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 929)

составлена на основании учебного плана:

09.03.01 ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

Направленность (профиль): Автоматизированные системы обработки информации и управления
утвержденного учебно-методическим советом вуза от 16.06.2022 протокол № 6.

Рабочая программа одобрена на заседании кафедры

Автоматизированных систем обработки информации и управления

Зав. кафедрой Профессор каф. АСОИУ, д.т.н., Бушмелева К.И.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование знаний об основных положениях теории и практики информационной безопасности.
1.2	Умений применять современные методы и средства защиты информации в вычислительных системах и сетях.
1.3	Применять знания, методы математического анализа и моделирования, теоретического и экспериментального исследования для оценки рисков информационной безопасности и организации противодействия угрозам.
1.4	Использовать современные информационные технологии и программные средства, в том числе отечественного производства, для защиты информации.
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.О.04
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	ЭВМ и периферийные устройства
2.1.2	Сети и телекоммуникации
2.1.3	Системное программное обеспечение
2.1.4	Математическая логика и теория алгоритмов
2.1.5	Алгоритмические языки программирования
2.2	Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Проектирование и эксплуатация АСОИУ
2.2.2	Производственная практика, преддипломная практика
2.2.3	Корпоративные информационные системы
3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
ОПК-3.1: Демонстрирует знания различных способов сбора, обработки и представления информации на основе информационной и библиографической культуры с учетом современных требований информационной безопасности	
ОПК-3.2: Использует различные информационно-коммуникационные технологии для решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры	
ОПК-2.1: Демонстрирует знания состава и функциональных возможностей современных информационных технологий и программных средств, в том числе отечественного производства, в части анализа, проектирования и разработки информационных и автоматизированных систем, при решении задач профессиональной деятельности	
ОПК-2.2: Выбирает и использует современные информационные технологии и программные средства, в том числе отечественного производства, на всех стадиях жизненного цикла информационных и автоматизированных систем, при решении задач профессиональной деятельности	
ОПК-2.3: Владеет способностью применять информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	
ОПК-1.1: Демонстрирует знания основ высшей математики, физики, инженерной графики, информатики, вычислительной техники, методов математического анализа, моделирования, программирования и проектирования, теоретического и экспериментального исследования в профессиональной деятельности	
ОПК-1.2: Решает стандартные профессиональные задачи с применением естественнонаучных и общинженерных знаний при проведении системного анализа и проектирования, применяет методы математического анализа и моделирования, использует результаты теоретического и экспериментального исследования в профессиональной деятельности	
ОПК-1.3: Владеет навыками выявления закономерностей информационных процессов, построения моделей, методами математического анализа, теоретического и экспериментального исследования объектов профессиональной деятельности	
В результате освоения дисциплины обучающийся должен	
3.1	Знать:
3.1.1	Базовый перечень методов и средств защиты компьютерной информации.
3.1.2	Различные способы сбора, обработки и представления информации на основе информационной и библиографической культуры с учетом современных требований информационной безопасности.
3.1.3	Состав и функциональные возможности современных информационных технологий и программных средств, в том числе отечественного производства, в части анализа, проектирования и разработки информационных и автоматизированных систем с учетом современных требований информационной безопасности.
3.1.4	Принципы классификации и примеры угроз безопасности компьютерным системам.
3.1.5	Методы использования знаний основ высшей математики, физики, инженерной графики, информатики, вычислительной техники, методов математического анализа, моделирования, программирования и проектирования, теоретического и экспериментального исследования в профессиональной деятельности.
3.1.6	Современные отечественные и международные стандарты информационной безопасности информационных систем.

3.2	Уметь:
3.2.1	Реализовывать методы криптографической защиты информации в вычислительных системах.
3.2.2	Использовать различные информационно-коммуникационные технологии для решения задач информационной безопасности на основе информационной и библиографической культуры.
3.2.3	Конфигурировать встроенные и дополнительные средства безопасности в операционной системе, локальных и глобальных сетях.
3.2.4	Выбирать и использовать современные информационные технологии и программные средства, в том числе отечественного производства, на всех стадиях жизненного цикла информационных и автоматизированных систем, при решении задач информационной безопасности.
3.2.5	Решать стандартные профессиональные задачи информационной безопасности с применением естественнонаучных и общеинженерных знаний.
3.2.6	Устанавливать и настраивать программное обеспечение для защиты компьютерной информации.
3.3	Владеть:
3.3.1	Методами аудита безопасности вычислительных систем.
3.3.2	Способностью применять информационные технологии и программные средства, в том числе отечественного производства, при решении задач информационной безопасности.
3.3.3	Навыками выявления закономерностей информационных процессов, построения моделей объектов профессиональной деятельности в части решения вопросов защиты информации.
3.3.4	Средствами обеспечения информационной безопасности и защиты данных вычислительных и информационных системах.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература	Примечание
	Раздел 1. Раздел 1					
1.1	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность защиты информации, связанной с составом и функциональными возможностями современных информационных технологий и программных средств. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.2	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации. Изучение различных информационно-коммуникационные технологии и их уровней безопасности. Факторы повышения уязвимости систем на всех стадиях жизненного цикла информационных и автоматизированных систем. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.3	Актуальность проблемы защиты информации. Основные факторы повышения уязвимости информации, связанных со способами сбора, обработки, представления информации и информационной культуры. Актуальность защиты информации, связанной с составом и функциональными возможностями современных информационных технологий и программных средств. /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.4	Основные понятия информационной безопасности и их связь со знаниями основ высшей математики, физики, информатики, вычислительной техники. Защиты информации и разработка информационных и автоматизированных систем, при решении задач профессиональной деятельности. Информационная культура и информационная безопасность. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.5	Основные понятия информационной безопасности. Основные подходы к созданию моделей информационной безопасности. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.6	Основные понятия информационной безопасности и их связь со знаниями основ высшей математики, физики, информатики, вычислительной техники. Защиты информации и разработка информационных и автоматизированных систем, при решении задач профессиональной деятельности. Информационная культура и информационная безопасность /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.7	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности. /Лек/	8	4	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.8	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Применение информационных технологий и программных средств, в том числе отечественного производства, и законодательное регулирование их применения /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.9	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности.. /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.10	Проблемы защиты информации в АСОИУ. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Лек/	8	2	ОПК-1.1 ОПК-1.2 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5

1.11	Проблемы защиты информации в АСОИУ. Информационные технологии и программные средства защиты информации в АСОИУ. /Лаб/	8	1	ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.12	Проблемы защиты информации в АСОИУ. Риски возникновения проблем защиты информации при проектировании и разработке информационных и автоматизированных систем. Различные способы сбора, обработки и представления информации с учетом современных требований информационной безопасности на всех уровнях жизненного цикла. /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.13	Содержание системы средств защиты компьютерной информации в АСОИУ. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.14	Содержание системы средств защиты компьютерной информации в АСОИУ. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.15	Содержание системы средств защиты компьютерной информации в АСОИУ. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.16	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ. Функции хэширования. Современные информационные технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5
1.17	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации в АСОИУ. Функции хэширования. Современные информационные технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Лаб/	8	2	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5

1.18	Симметричные и асимметричные криптосистемы для защиты компьютерной информации в АСОИУ. Функции хэширования. Современные информационных технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования.	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.19	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.20	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.21	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Ср/	8	4	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.22	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.23	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.24	Защита компьютерных систем от удаленных атак через сеть Internet. Программные и технические средства противодействия сетевым атакам. Технологии и методы борьбы с угрозами в сети Intenet. /Ср/	8	2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.25	Подготовка реферата /Реф/	8	0	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Подготовка доклада и презентации по теме реферата

1.26	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.27	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.28	Методы защиты программ от изучения и разрушающих программных воздействий (программных закладок и вирусов). Программные и технические средства противодействия вредоносному ПО. Технологии и методы борьбы с угрозами от воздействия вредоносного ПО /Ср/	8	2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.29	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.30	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.31	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Ср/	8	2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.32	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Лек/	8	2	ОПК-1.1 ОПК-2.1 ОПК-3.1	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.33	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты /Лаб/	8	1	ОПК-1.2 ОПК-1.3 ОПК-2.2 ОПК-2.3 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	

1.34	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Ср/	8	2	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.35	Контрольная работа /Контр.раб./	8	0	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Выполнение контрольной работы
1.36	Зачёт /Зачёт/	8	0	ОПК-1.1 ОПК-1.2 ОПК-1.3 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-3.1 ОПК-3.2	Л1.1 Л1.2 Л1.3 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Устный опрос на зачете

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1. Контрольные вопросы и задания

Представлено отдельным документом

5.2. Темы письменных работ

Представлено отдельным документом

5.3. Фонд оценочных средств



Представлено отдельным документом

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л1.1	Башлы П. Н.	Информационная безопасность и защита информации	Москва: Издательский Центр РИО❖, 2013, электронный ресурс	1
Л1.2	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО❖, 2017, электронный ресурс	1
Л1.3	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017, электронный ресурс	1
Л1.4	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО❖, 2018, электронный ресурс	1
Л1.5	Баранова Е.К., Бабаш А.В.	❖Информационная безопасность и защита информации: Учебное пособие	Москва: ❖Издательский Центр Р❖О❖, 2019, электронный ресурс	1

Л1.6	Щеглов А. Ю., Щеглов К. А.	Защита информации: основы теории: Учебник	Москва:  Издательство Юрайт, 2020, электронный ресурс	1
6.1.2. Дополнительная литература				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.1	Братановский С. Н., Лапин С. Ю.	Обеспечение доступа граждан к информации о деятельности органов государственной власти и местного самоуправления в Российской Федерации. Информационно-правовой аспект: Монография	Саратов: Электронно-библиотечная система IPRbooks, 2012, электронный ресурс	1
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л2.2	Гультяева Т. А.	Основы теории информации и криптографии: Конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, электронный ресурс	1
Л2.3	Бухтояров В. В., Золотарев В. В., Жуков В. Г.	Поддержка принятия решений при проектировании систем защиты информации: Монография	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014, электронный ресурс	1
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Колич-во
Л3.1	Жук А. П., Жук Е. П., Лепешкин О. М., Тимошкин А. И.	Защита информации: Учебное пособие	Москва: Издательский Центр РИО  , 2015, электронный ресурс	1
Л3.2	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: Издательство "ФОРУМ", 2015, электронный ресурс	1
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	российский общеобразовательный портал			
Э2	электронный журнал Открытые системы			
Э3	сайт Информационных технологий			
Э4	интернет-издание, посвященное новостям компьютерной индустрии, науки и техники.			
Э5	журнал для ИТ-профессионалов.			
6.3.1 Перечень программного обеспечения				
6.3.1.1	MS Office			
6.3.1.2	MS Visual Studio 2019			
6.3.2 Перечень информационных справочных систем				
6.3.2.1	Гарант-информационно-правовой портал. http://www.garant.ru/			
6.3.2.2	КонсультантПлюс –надежная правовая поддержка. http://www.consultant.ru/			
7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)				
7.1	аудитория, оборудованная техническими средствами для демонстрации лекций-визуализаций;			
7.2	лабораторные работы должны выполняться в специализированных классах, оснащенных современными персональными компьютерами, включенными в сеть и программным обеспечением, в соответствии с тематикой изучаемого материала;			
7.3	число рабочих мест в классах должно быть таким, чтобы обеспечивалась индивидуальная работа студента на отдельном персональном компьютере.			