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

Методы защиты информации

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Автоматизированных систем обработки информации и управления**

Учебный план b010302-ПМ-22-4.plx
Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА
Направленность (профиль): Прикладная математика и информатика

Квалификация **бакалавр**

Форма обучения **очная**

Общая трудоемкость **3 ЗЕТ**

Часов по учебному плану 108
в том числе:
аудиторные занятия 48
самостоятельная работа 24
часов на контроль 36

Виды контроля в семестрах:
экзамены 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	17 3/6			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Практические	16	16	16	16
Итого ауд.	48	48	48	48
Контактная работа	48	48	48	48
Сам. работа	24	24	24	24
Часы на контроль	36	36	36	36
Итого	108	108	108	108

Программу составил(и):
Доцент, Гавриленко Т.В.

Рабочая программа дисциплины
Методы защиты информации

разработана в соответствии с ФГОС:
Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 01.03.02 Прикладная математика и информатика (приказ Минобрнауки России от 10.01.2018 г. № 9)

составлена на основании учебного плана:
Направление 01.03.02 ПРИКЛАДНАЯ МАТЕМАТИКА И ИНФОРМАТИКА
Направленность (профиль): Прикладная математика и информатика
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 Бушмелева К.И.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ	
1.1	Формирование у обучающихся знаний об основных положениях теории и практики информационной безопасности.
1.2	Формирование у обучающихся умений применять современные методы и средства защиты информации в вычислительных системах и сетях
1.3	Формирование способности использовать современные информационные технологии и программные средства, в том числе отечественного производства, для защиты информации.
1.4	Формирование у обучающихся способности разрабатывать программное обеспечение и процедуры интеграции программных модулей, с учетом требований информационной безопасности.
1.5	Формирование способности осуществлять интеграцию программных модулей и компонент и верификацию выпусков программного продукта, с учетом требований информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП	
Цикл (раздел) ООП:	Б1.В.ДВ.03
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Объектно-ориентированное программирование
2.1.2	Информатика
2.1.3	Базы данных
2.1.4	Программирование на СИ
2.1.5	Иностранный язык
2.1.6	Иностранный язык в профессиональной сфере
2.1.7	Основы программирования
2.1.8	Разработка программного обеспечения в ОС Linux
2.1.9	Безопасность жизнедеятельности
2.1.10	Дискретная математика
2.1.11	Алгоритмы и методы программирования
2.1.12	Операционные системы
2.2	**Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Технологии параллельного программирования
2.2.2	Производственная практика, преддипломная практика
2.2.3	Производственная практика, научно-исследовательская работа
2.2.4	Системное программное обеспечение
2.2.5	Сети ЭВМ
2.2.6	Выполнение и защита выпускной квалификационной работы
2.2.7	Геоинформационные технологии
2.2.8	Изобретательская деятельность

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)
ПК-4.1: Выполняет процедуры сборки программных модулей и компонент в программный продукт

ПК-4.2: Проводит оценку работоспособности программного продукта

ПК-3.1: Разрабатывает программное обеспечение, используя современные среды программирования

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**

3.1.1	Базовый перечень методов и средств защиты компьютерной информации.
3.1.2	Принципы классификации и примеры угроз безопасности компьютерным системам.
3.1.3	Современные отечественные и международные стандарты информационной безопасности информационных систем.
3.1.4	Методы, подходы и процедуры сборки программных модулей и компонент в программный продукт с учетом требований информационной безопасности.
3.1.5	Методы оценки работоспособности программного продукта с учетом требований информационной безопасности.
3.1.6	Подходы к разработке программного обеспечения, используя современные среды программирования с учетом требований информационной безопасности.
3.2	**Уметь:**
3.2.1	Выполнять процедуры сборки программных модулей и компонент криптографической защиты информации в вычислительных системах.
3.2.2	Конфигурировать встроенные и дополнительные средства безопасности в операционной системе, локальных и глобальных сетях.
3.2.3	Устанавливать и настраивать программное обеспечение для защиты компьютерной информации.
3.2.4	Проводить оценку работоспособности программного продукта с учётом требований информационной безопасности
3.2.5	Разрабатывать программное обеспечение используя современные среды программирования, с учетом требований информационной безопасности
3.3	**Владеть:**
3.3.1	Методами аудита безопасности вычислительных систем;
3.3.2	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	Компетен-ции	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/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.2	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. /Пр/	7	1	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.3	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/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	

1.4	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/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.5	Основные понятия информационной безопасности. Основные подходы к созданию моделей информационной безопасности. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.6	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/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.7	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности. /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.8	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. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.9	Законодательные и правовые основы защиты компьютерной информации информационных технологий. Библиографическая культура с учетом современных требований информационной безопасности. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	

1.10	Проблемы защиты информации. 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/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.11	Проблемы защиты информации. Информационные технологии и программные средства защиты информации. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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. 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/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.13	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.14	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.15	Содержание системы средств защиты компьютерной информации. Анализ средств защиты информации при проектировании и разработке информационных и автоматизированных систем. Применение теоретического и экспериментального исследования для выявления рисков. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.16	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационных технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	

1.17	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационных технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.18	Симметричные и ассиметричные криптосистемы для защиты компьютерной информации. Функции хэширования. Современные информационных технологии и программные средства, в том числе отечественного производства, реализующие криптографические системы и функции хэширования. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.19	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.20	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.21	Идентификация, аутентификация, авторизация. Методы аутентификации и представление аутентификационной информации на основе информационной культуры с учетом современных требований информационной безопасности. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 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/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.23	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. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	

1.24	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/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.25	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/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.26	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. /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.27	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. /Ср/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.28	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты. /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.29	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.30	Методы и средства защиты носителей информации. Защита информационных ресурсов от несанкционированного доступа. Технологии программирования и подходы к реализации систем защиты /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	

1.31	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Лек/	7	3	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.32	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты /Пр/	7	1,5	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.33	Основные виды атак на протоколы аутентификации. Основные приемы предотвращения атак. Программные средства защиты. /Ср/	7	2	ПК-3.1 ПК-4.1 ПК-4.2	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	
1.34	/Контр.раб./	7	0	ПК-3.1 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6Л2.1 Л2.2 Л2.3Л3.1 Л3.2	
1.35	Экзамен /Экзамен/	7	36	ПК-3.1 ПК-4.1 ПК-4.2	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	

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

	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	Внуков А. А.	Основы информационной безопасности: защита информации: Учебное пособие	Москва: Издательство Юрайт, 2019, электронный ресурс	1
Л1.6	Хорев П. Б.	Программно-аппаратная защита информации: Учебное пособие	Москва: ООО "Научно-издательский центр ?НФРА- М", 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
Л2.2	Гультяева Т. А.	Основы теории информации и криптографии: Конспект лекций	Новосибирск: Новосибирский государственный технический университет, 2010, электронный ресурс	1

	Авторы, составители	Заглавие	Издательство, год	Колич-во
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	Пакет прикладных программ Microsoft Office,			
6.3.1.2	Операционная система Windows,			
6.3.1.3	Microsift Visual Studio 2019			
6.3.2 Перечень информационных справочных систем				
6.3.2.1	http://www.garant.ru Информационно-правовой портал Гарант.ру			
6.3.2.2	http://www.consultant.ru/ Справочно-правовая система Консультант Плюс			

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
7.1	Учебные аудитории для проведения занятий лекционного типа, групповых и индивидуальных консультаций, укомплектованные специализированной мебелью и техническими средствами обучения (доска, экран (стационарный или переносной), проектор (стационарный или переносной)).
7.2	Учебные аудитории для проведения практических занятий - компьютерный класс, оборудованный техникой (персональные компьютеры, локальная вычислительная сеть с выходом в глобальную сеть Internet и доступом в электронную информационно-образовательную среду организации) из расчета один компьютер на одного обучающегося, с обустроенным рабочим местом преподавателя.
7.3	Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечения доступа в электронную информационно-образовательную среду организации.