ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"
(ФГБОУ ВО УрГУПС)

Б1.Б.23 Безопасность сетей ЭВМ

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационные технологии и защита информации**

Учебный план 10.03.01 ИБ-2021.plx
10.03.01 Информационная безопасность

Направленность (профиль) Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **7 ЗЕТ**

Часов по учебному плану 252
в том числе:
аудиторные занятия 108
самостоятельная работа 108
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 5 зачет с оценкой 6

Часов контактной работы всего, в том числе: 116,15
аудиторная работа 108
текущие консультации по лабораторным занятиям 5,4
консультации перед экзаменом 2
прием экзамена 0,5
прием зачета с оценкой 0,25

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		**6 (3.2)**		Итого	
Недель	18		18			
Вид занятий	УП	РП	УП	РП	УП	РП
Лекции	36	36	18	18	54	54
Лабораторные	18	18	36	36	54	54
Итого ауд.	54	54	54	54	108	108
Контактная работа	54	54	54	54	108	108
Сам. работа	54	54	54	54	108	108
Часы на контроль	36	36			36	36
Итого	144	144	108	108	252	252

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: Теоретическая и практическая подготовка выпускников в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.
1.2	Задачи дисциплины: Изучение основ администрирования вычислительных сетей; формирование навыков настройки политики безопасности вычислительных сетей, применения средств защиты информации в вычислительных сетях.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	Б1.Б

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения дисциплин Информатика и аппаратные средства вычислительной техники, Сети и системы передачи информации, Методы и средства криптографической защиты информации.
В результате освоения предшествующей дисциплины обучающийся должен знать: эталонную модель взаимодействия открытых систем; методы коммутации и маршрутизации, сетевые протоколы; сигналы электросвязи, принципы построения систем и средств связи;
уметь: формулировать и настраивать политику безопасности распространения операционных систем, а также локальных вычислительных сетей, построенных на их основе;
владеть: навыками анализа основных нормативных правовых актов в области информационной безопасности и защиты программирования информации, а также нормативные методические документы Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области.

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Защита информационных процессов на транспорте
Комплексные системы защиты информации на транспорте
Программно-аппаратные средства защиты информации
Производственная практика (технологическая практика)
Управление информационной безопасностью на объектах транспортной инфраструктуры
Подготовка к процедуре защиты и защита выпускной квалификационной работы
Подготовка к сдаче и сдача государственного экзамена
Производственная практика (преддипломная практика)
Производственная практика (эксплуатационная практика)

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-2.2: Знает и применяет информационно-коммуникационные технологии, принципы организации информационных систем и сетей в соответствии с требованиями по защите информации для решения задач профессиональной деятельности
ОПК-2.3: Осуществляет меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты информации
ОПК-2.1: Знает аппаратные средства вычислительной техники, принципы построения информационных систем и сетей, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
ОПК(п)-2.2: Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ОПК(п)-2.2.1: Знает методы деструктивных воздействия на информационные ресурсы
ОПК(п)-2.2.2: Знает методы оценки устойчивости объектов защиты к деструктивным воздействиям на информационные ресурсы
ОПК(п)-2.2.3: Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	основы администрирования вычислительных сетей.
3.2	**Уметь:**

3.2.1	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе;
3.2.2	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
3.3	**Владеть:**
3.3.1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
3.3.2	навыками выявления и уничтожения компьютерных вирусов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Основные понятия и анализ угроз информационной безопасности					
1.1	Принципы многоуровневой защиты корпоративной информации /Лек/	5	4	ОПК-2.1 ОПК-2.2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
1.2	Основы сетевого и межсетевого взаимодействия /Лек/	5	4	ОПК-2.1 ОПК-2.2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
1.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК-2.1 ОПК-2.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
	Раздел 2. Политика информационной безопасности					
2.1	Политика безопасности. Структура политики безопасности /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.3 ОПК-5.2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
2.2	Стандарты информационной безопасности /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.3 ОПК-5.2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
2.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК(п)-2.2.1 ОПК(п)-2.2.3 ОПК-5.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
2.4	Классификация и анализ угроз информационной безопасности /Лаб/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК-5.2	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение классификации
2.5	Подготовка отчета по лабораторной работе /Ср/	5	8	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК-5.2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
	Раздел 3. Криптографическая защита информации					
3.1	Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	

3.2	Управление крипто ключами и открытыми ключами PKI /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
3.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
3.4	Передача шифрованных данных с помощью квантовой криптографии /Лаб/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
3.5	Подготовка отчета по лабораторной работе /Ср/	5	8	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
	Раздел 4. Идентификация, аутентификация и управление доступом					
4.1	Идентификация, аутентификация и управление доступом /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
4.2	Управление доступом по схеме однократного входа с авторизацией Single Sign-On /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
4.3	Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса. /Лек/	5	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	

4.4	Модель OSI. Сетевые протоколы. Стек протоколов TCP/IP /Лаб/	5	2	ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
4.5	Автоматизация процесса создания учетных записей пользователей в операционных системах Windows.Создание скриптов автозапуска идентификационной информации. /Лаб/	5	4	ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
4.6	Знакомство со средой виртуализации VMWare. Создание виртуальной сетевой инфраструктуры /Лаб/	5	4	ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
4.7	Подготовка отчета по лабораторной работе /Ср/	5	8	ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
4.8	Промежуточная аттестация /Экзамен/	5	36	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
	Раздел 5. Многоуровневая защита корпоративных информационных систем					
5.1	Корпоративная информационная система /Лек/	6	2	ОПК-5.2 ОПК-2.1 ОПК-2.2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
5.2	Сети периметра и стратегии удаленного доступа /Лек/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
5.3	Доменная сеть на основе Windows Server. Создание и настройка контроллеров домена /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.4	Доменная сеть на основе Windows Server создание и настройка клиентских машин /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.5	Файловая система и локальные диски. /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
5.6	Создание динамического массива для хранения данных. RAID технологии. /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии

5.7	Конфигурирование инфраструктуры DHCP на основе операционной системы Windows Server /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э2	Работа в малых группах. Освоение программного обеспечения
5.8	Создание пользовательских групп посредством скриптов. Настройка безопасности сети и разграничение доступа к ресурсам /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.9	Создание пользовательских групп посредством графического интерфейса. Настройка безопасности сети и разграничение доступа к ресурсам /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.10	Настройка политики паролей и блокировки пользователей /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.11	Установка службы DNS /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
5.12	Защита серверного и клиентского программного обеспечения посредством групповой политики безопасности /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
5.13	Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем /Лек/	6	2	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
5.14	Изучение литературы по тематике раздела /Ср/	6	6	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
5.15	Управление программным обеспечением с помощью групповой политики /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
5.16	Перемещаемые профили, квотирование, блокировка файлов /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
5.17	Репликация и разделы каталога /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии

5.18	Подготовка отчетов по лабораторным работам /Ср/	6	10	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
	Раздел 6. Протоколы защищенных каналов					
6.1	Модель взаимодействия систем стек протоколов TCP/IP /Лек/	6	2	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
6.2	Защита на сетевом и сеансовом уровнях – протоколы IPSec, SSL, TSL, SOCKS. /Лек/	6	2	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
6.3	Защита на канальном уровне – протоколы удаленного доступа /Ср/	6	2	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
6.4	Изучение литературы и нормативных документов по тематике раздела /Ср/	6	6	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
6.5	Мониторинг сетевой структуры /Лаб/	6	2	ОПК(п)-2.2.2 ОПК (п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение технологии
6.6	Защита сети посредством установки и настройки межсетевого экрана /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
6.7	Создание VPN туннеля для удаленного подключения пользователей к защищенной сети /Лаб/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения
6.8	Подготовка отчетов по лабораторным работам /Ср/	6	4	ОПК(п)-2.2.2 ОПК (п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	

	Раздел 7. Технологии межсетевого экранирования					
7.1	Функционирование межсетевых экранов на различных уровнях модели OSI /Лек/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
7.2	Схемы сетевой защиты на базе межсетевых экранов /Лек/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
7.3	Виртуальные частные сети /Лек/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
7.4	Подготовка отчета по лабораторной работе /Ср/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
	Раздел 8. Управление информационной безопасностью					
8.1	Управление рисками информационной безопасности. Аудит безопасности информационных систем /Лек/	6	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2	
8.2	Изучение литературы по тематике раздела /Ср/	6	10	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
8.3	Установка сервера обновлений WSUS+MS SQL сервер. Установка и конфигурирование сервера антивирусной защиты локальной сети /Лаб/	6	4	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.2 Э1 Э2	Работа в малых группах. Освоение программного обеспечения

8.4	Подготовка отчетов по лабораторным работам /Ср/	6	2	ОПК(п)-2.2.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	
8.5	Подготовка к промежуточной аттестации /Ср/	6	12	ОПК(п)-2.2.1 ОПК (п)-2.2.2 ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Э1 Э2	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.
Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

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

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1.1. Основная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Гузенкова Е. А.	Безопасность сетей ЭВМ: конспект лекций для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л1.2	Шаньгин В.Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020	http://znanium.com

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020	http://znanium.com
Л2.2	Шелухин О. И., Сакалема Д. Ж., Филинова А. С.	Обнаружение вторжений в компьютерные сети (сетевые аномалии)	Москва: Горячая линия -Телеком, 2018	http://e.lanbook.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А.	Безопасность сетей ЭВМ: методические рекомендации по дисциплине «Безопасность сетей ЭВМ» к самостоятельной работе студентов направления подготовки 10.03.01 - «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Гузенкова Е. А.	Безопасность сетей ЭВМ: методические указания к лабораторным работам по дисциплине «Безопасность сетей ЭВМ» для студентов направления подготовки 10.03.01 - «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)	
Э1	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)
Э2	Официальный сайт ОАО "Российские железные дороги" (http://www.rzd.ru)
6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем	
6.3.1 Перечень программного обеспечения	
6.3.1.1	Неисключительные права на ПО Windows
6.3.1.2	Неисключительные права на ПО Office
6.3.1.3	Программное обеспечение компьютерного тестирования АСТ
6.3.1.4	Операционная система Astra Linux
6.3.1.5	Серверная операционная система: Windows Server
6.3.1.6	Система электронной поддержки обучения Blackboard Learn
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Справочно-правовая система КонсультантПлюс
6.3.2.2	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.3	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
6.3.2.4	Международная реферативная база данных научных изданий Scopus
6.3.2.5	Международная реферативная база данных научных изданий eLIBRARY.RU
6.3.2.6	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.7	Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Назначение	Оснащение
Лаборатория «Программно-аппаратные средства защищенных информационных систем». Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе киптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппартные средства аутетификации пользователя Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель Моноблоки с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения текущего	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, включая ПО АСТ-Тест, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную

контроля и промежуточной аттестации	информационно-образовательную среду Университета
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования
Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Эффективное освоение дисциплины предполагает регулярное посещение всех видов аудиторных занятий, выполнение плана самостоятельной работы в полном объеме и прохождение аттестации в соответствии с календарным учебным графиком. Обучающемуся рекомендуется ознакомиться со списком основной и дополнительной литературы и взять в библиотеке издания (необходимо иметь при себе персонифицированную электронную карту и уметь пользоваться электронным каталогом «ИРБИС»).Доступ к информационным ресурсам библиотеки и информационно-справочным системам сети «Интернет» организован в читальных залах библиотеки, в компьютерных классах, в помещениях для самостоятельной работы обучающихся со стационарных ПЭВМ, либо с личного ПЭВМ (ноутбука, планшетного компьютера или иного мобильного устройства) посредством беспроводного доступа при активации индивидуальной учетной записи. Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий. Комплект учебно-методических материалов по всем видам учебной деятельности, предусмотренным рабочей программой дисциплины (модуля), размещен на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося. Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя:- изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий);- подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".Перечень учебно-методических материалов (учебно-методического обеспечения) для самостоятельной работы обучающихся по дисциплине указан по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)", материалы размещены на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru).

При применении дистанционных образовательных технологий и электронного обучения освоение дисциплины (модуля) осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru)) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.