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-2020.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Направленность (профиль) направленность (профиль) N 2 "Организация и технология 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	РПД	УП	РПД	УП	РПД
Лекции	36	36	18	18	54	54
Лабораторные	18	18	36	36	54	54
Контактная работа	54	54	54	54	108	108
Итого ауд.	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. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Теоретическая и практическая подготовка выпускников в области построения сетей ЭВМ и обеспечения безопасности при эксплуатации сетей ЭВМ.

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, Криптографические методы 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:

Комплексные системы защиты информации на транспорте
Защита информационных процессов на транспорте
Программно-аппаратные средства защиты информации
Учебная практика (ознакомительная практика)
Учебная практика (практика по получению первичных профессиональных умений и навыков)
Учебная практика (технологическая практика)
Производственная практика (проектно-технологическая практика)
Производственная практика (эксплуатационная практика)
Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОПК-7: способностью определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты	
Знать:	
Уровень 1	классификацию информации, подлежащей защите
Уровень 2	классификацию угроз информационной безопасности
Уровень 3	виды и возможные методы реализации угроз информационной безопасти
Уметь:	
Уровень 1	определять виды и формы информации, подверженной угрозам
Уровень 2	анализировать структуру и содержания информационных процессов предприятия
Уровень 3	определять виды и возможные пути реализации угроз информационной безопасности
Владеть:	
Уровень 1	навыками определения видов и форм информации, подверженной угрозам
Уровень 2	навыками анализа структуры и содержания информационных процессов предприятия
Уровень 3	навыками определения видов и возможных путей реализации угроз информационной безопасности

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации	
Знать:	
Уровень 1	особенности установки, настройке и обслуживания программных, программно-аппаратных средств защиты информации
Уровень 2	способы формирования инструкций для настройки программных, программно-аппаратных средств в защищенном исполнении
Уровень 3	принципы реализации настроек программных, программно-аппрататных средств в соотвествии с разработанной политикой безопасности на предприятии
Уметь:	
Уровень 1	производить настройку основного программных, программно-аппаратных средств защиты информации
Уровень 2	производить настройку программных, программно-аппаратных средств в соотвествии с документацией по информационной безопасности
Уровень 3	производить комплексную настройку программных, программно-аппаратных средств защиты информации

	и устранять конфликты в комплексной работе различных систем
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	производить выбор программных средств системного, прикладного назначения для реализации защиты информации
Уровень 2	создавать инструкции по применению различных программных средств в комплексной реализации защиты информации
Уровень 3	создавать дополнительные программные средства, для решения возникающих конфликтов между различными средствами защиты информации, применяемых в одной информационной системе
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	методологию администрирования вычислительных сетей
Уровень 2	механизмы администрирования, тенденции их развития (управление распределением памяти для объектов ИС, установление квот памяти для пользователей ИС, управление доступностью данных, вулючая режимы
Уровень 3	методы анализа информационных систем, модели представления проетных решений, конфигурации информационных систем, структуру, принципы реализации и функционирования информационных технологий, используемых при создании информационных систем, базовые и прикладные информационные технологии, инструментальные средства информационных технологий, состав свойств готовых компонентов, принципы адаптации.
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распределенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
Уровень 2	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Уровень 3	давать оценку конфигурационным свойсвам системы и составлять рекомендации по ее маштабированию и защите
Владеть:	
Уровень 1	методикой анализа современных информационных вычислительных сетей
Уровень 2	методикой анализа новых технологий и возможностью реализации их на предприятии
Уровень 3	методикой оценки эффективности работы сетевой среды и методами оптимизации основных ее показателей

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знать:	
Уровень 1	основы администрирования вычислительных сетей
Уровень 2	механизмы администрирования, тенденции их развития (управление распределением памяти для объектов ИС, установление квот памяти для пользователей ИС, управления доступностью данных, включая режимы (состояния))
Уровень 3	методы анализа информационных систем, модели представления проектных решений, конфигурации информационных систем; структуру, принципы реализации и функционирования информационных технологий, используемых при создании информационных систем, базовые и прикладные информационные технологии, инструментальные средства информационных технологий, состав и свойств готовых компонентов, принципы их адаптации
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе

Уровень 2	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Уровень 3	оценить конфигурацию системы и дать рекомендации по усилению мер защиты
Владеть:	
Уровень 1	навыками выявления и уничтожения компьютерных вирусов
Уровень 2	методикой анализа сетевого трафика
Уровень 3	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений

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-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
1.2	Основы сетевого и межсетевого взаимодействия /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
1.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
	Раздел 2. Политика информационной безопасности					
2.1	Политика безопасности. Структура политики безопасности /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
2.2	Стандарты информационной безопасности /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	

2.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4	Л1.1 Л1.2 Л2. Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
2.4	Классификация и анализ угроз информационной безопасности /Лаб/	5	4	ОПК-7 ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
2.5	Подготовка отчета по лабораторной работе /Ср/	5	8	ОПК-7 ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
	Раздел 3. Криптографическая защита информации					
3.1	Симметричные и ассиметричные системы шифрования. Функции хеширования. Электронная подпись /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2	
3.2	Управление крипто ключами и открытыми ключами PKI /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Э1 Э2	
3.3	Изучение литературы по тематике раздела /Ср/	5	10	ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
3.4	Передача шифрованных данных с помощью квантовой криптографии /Лаб/	5	4	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.2 Л2.3 Л2.4 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
3.5	Подготовка отчета по лабораторной работе /Ср/	5	8	ОПК-7 ПК-3 ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
	Раздел 4. Идентификация, аутентификация и управление доступом					

4.1	Идентификация, аутентификация и управление доступом /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
4.2	Управление доступом по схеме однократного входа с авторизацией Single Sign-On /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
4.3	Доменные службы Active Directory. Структуры леса, доменных деревьев. Проектирование отношений и оптимизация аутентификации внутри леса. /Лек/	5	4	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
4.4	Модель OSI. Сетевые протоколы. Стек протоколов TCP/IP /Лаб/	5	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
4.5	Автоматизация процесса создания учетных записей пользователей в операционных системах Windows.Создание скриптов автозапуска идентификационной информации. /Лаб/	5	4	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
4.6	Знакомство со средой виртуализации VMWare. Создание виртуальной сетевой инфраструктуры /Лаб/	5	4	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
4.7	Подготовка отчета по лабораторной работе /Ср/	5	8	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
4.8	Промежуточная аттестация /Экзамен/	5	36	ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л3.1 Л3.2 Э1 Э2	
	Раздел 5. Многоуровневая защита корпоративных информационных систем					
5.1	Корпоративная информационная система /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
5.2	Сети периметра и стратегии удаленного доступа /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
5.3	Доменная сеть на основе Windows Server. Создание и настройка контроллеров домена /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач

5.4	Доменная сеть на основе Windows Server создание и настройка клиентских машин /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.5	Файловая система и локальные диски. /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
5.6	Создание динамического массива для хранения данных. RAID технологии. /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.7	Конфигурирование инфраструктуры DHCP на основе операционной системы Windows Server /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э2	Решение практико-ориентированных задач
5.8	Создание пользовательских групп посредством скриптов. Настройка безопасности сети и разграничение доступа к ресурсам /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1Л2.1 Л2.3 Л2.4 Л2.5 Л2.6Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.9	Создание пользовательских групп посредством графического интерфейса. Настройка безопасности сети и разграничение доступа к ресурсам /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.10	Настройка политики паролей и блокировки /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1Л2.1 Л2.3 Л2.4 Л2.5 Л2.6Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.11	Установка службы DNS /Лаб/	6	2	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач
5.12	Защита серверного и клиентского программного обеспечения посредством групповой политики безопасности /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	
5.13	Обеспечение безопасности операционных систем. Локальные политики безопасности. Встроенные системы защиты операционных систем /Лек/	6	2	ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
5.14	Изучение литературы по тематике раздела /Ср/	6	6	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
5.15	Управление программным обеспечением с помощью групповой политики /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач

5.16	Перемещаемые профили, квотирование, блокировка файлов /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
5.17	Репликация и разделы каталога /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
5.18	Подготовка отчетов по лабораторным работам /Ср/	6	10	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
	Раздел 6. Протоколы защищенных каналов					
6.1	Модель взаимодействия систем стек протоколов TCP/IP /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
6.2	Защита на сетевом и сеансовом уровнях – протоколы IPSec, SSL, TSL, SOCKS. /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
6.3	Защита на канальном уровне – протоколы удаленного доступа /Ср/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
6.4	Изучение литературы и нормативных документов по тематике раздела /Ср/	6	6	ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2	
6.5	Мониторинг сетевой структуры /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
6.6	Защита сети посредством установки и настройки межсетевого экрана /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Работа в малых группах, анализ практико-ориентированных задач
6.7	Создание VPN туннеля для удаленного подключения пользователей к защищенной сети /Лаб/	6	2	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач

6.8	Подготовка отчетов по лабораторным работам /Ср/	6	4	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
	Раздел 7. Технологии межсетевого экранирования					
7.1	Функционирование межсетевых экранов на различных уровнях модели OSI /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
7.2	Схемы сетевой защиты на базе межсетевых экранов /Лек/	6	2	ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
7.3	Виртуальные частные сети /Лек/	6	2	ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
7.4	Подготовка отчета по лабораторной работе /Ср/	6	2	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	
	Раздел 8. Управление информационной безопасностью					
8.1	Управление рисками. Аудит безопасности ИС /Лек/	6	2	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Э1 Э2	
8.2	Изучение литературы по тематике раздела /Ср/	6	10	ОПК-7 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Э1 Э2	
8.3	Установка сервера обновлений WSUS+MS SQL сервер. Установка и конфигурирование сервера антивирусной защиты локальной сети /Лаб/	6	4	ПК-1 ПК-2 ПК-3	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л3.2 Э1 Э2	Решение практико-ориентированных задач
8.4	Подготовка отчетов по лабораторным работам /Ср/	6	2	ПК-4	Л1.1 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 Э1 Э2	

8.5	Подготовка к промежуточной аттестации /Ср/	6	12	ОПК-7 ПК-1 ПК-2 ПК-3 ПК-4	Л1.1 Л1.2 Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Л3.2 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	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2018	http://znanium.com
Л1.2	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

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Шелухин О. И., Сакалема Д. Ж., Филинова А. С., Шелухин О. И.	Обнаружение вторжений в компьютерные сети: (сетевые аномалии) : рекомендовано УМО по образованию в области Инфокоммуникационных технологий и систем связи в качестве учебного пособия для студентов высших учебных заведений, обучающихся по направлению подготовки 210700 - «Инфокоммуникационные технологии и системы связи» квалификации (степени) "бакалавр" и квалификации (степени) "магистр"	Москва: Горячая линия - Телеком, 2018	http://e.lanbook.com
Л2.2	Бабаш А. В.	Криптографические методы защиты информации. Том 3: Учебно-методическое пособие	Москва: Издательский Центр РИО, 2014	http://znanium.com
Л2.3	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017	http://znanium.com
Л2.4	Максимов Н. В., Попов И. И.	Компьютерные сети: Учебное пособие для студентов учреждений среднего профессионального образования	Москва: Издательство "ФОРУМ", 2017	http://znanium.com
Л2.5	Кузин А. В., Кузин Д.А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2018	http://znanium.com

Л2.6		ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология: официальное издание	Москва: Стандартинформ, 2014	http://gostexpert.ru/gost/gost-27000-2012#text
Л2.7		ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: официальное издание	Москва: Стандартинформ, 2008	http://gostexpert.ru/gost/gost-27001-2006#text
Л2.8		ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности: официальное издание	Москва: Стандартинформ, 2014	http://gostexpert.ru/gost/gost-27002-2012#text
Л2.9		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.10		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.11		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.12		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist
Л2.13		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist
Л2.14		Каталог учебных, учебно-методических пособий, научных и других изданий вузов железнодорожного транспорта: справочно-библиографическое издание	Москва, ФГБУ ДПО «УМЦ ЖДТ» 2018	http://www.usurt.ru/izdatelsko-bibliotechnyy-kompleks/bibliotechno-informacionnuy-center/katalog-fgbou-umts-zhdt
Правовые нормативные акты и нормативные методические документы в области информационной безопасности при изучении данной дисциплины не используются				

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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
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". Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе криптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппаратные средства аутентификации 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 контроля и промежуточной аттестации	Специализированная мебель Компьютерная техника 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 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.

Студенту 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 студентов 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.

Формы самостоятельной работы студентов по данной дисциплине разнообразны. Они включают в себя:

- изучение лекционного и дополнительного материала (учебной, научной, методической литературы, материалов периодических изданий);
- подготовку к занятиям, предусмотренных РПД, мероприятиям текущего контроля и промежуточной аттестации

Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности.

При выполнении самостоятельной работы студент должен руководствоваться методическими указаниями, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для СРС по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".

Перечень 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).