ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.В.ДВ.04.02 Защита информационных процессов на транспорте

рабочая программа дисциплины (модуля)

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

Учебный план 10.03.01 ИБ-2023.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) **5 ЗЕТ**

Часов по учебному плану 180
в том числе:
аудиторные занятия 54
самостоятельная работа 72
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 7

Часов контактной работы всего, в том числе: 60,1
аудиторная работа 54
текущие консультации по практическим занятиям 3,6
консультации перед экзаменом 2
прием экзамена 0,5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	36	36	36	36
Элект	18	18	18	18
Итого ауд.	54	54	54	54
Контактная работа	72	72	72	72
Сам. работа	72	72	72	72
Часы на контроль	36	36	36	36
Итого	180	180	180	180

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: Формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.
1.2	Задачи дисциплины: Изучение основных аспектов деятельности по созданию, обеспечению функционирования и контролю эффективности комплексной системы защиты информации на предприятии. Изучение структуры комплексной системы защиты информации на предприятии. Обобщение основополагающих нормативно-правовых принципов организации системы защиты информации.
1.3	Изучение методов проведения анализа и управления информационными рисками предприятия.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	Б1.В.ДВ.04

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные при изучении дисциплин Теория информации, Организационное и правовое обеспечение информационной безопасности, Безопасность информационных процессов, Безопасность сетей ЭВМ, Теория информационной безопасности и методология защиты информации, Стеганография.
В результате освоения предшествующих дисциплин обучающийся должен знать: принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; принципы построения информационных систем; принципы организации информационных систем в соответствии с требованиями по защите информации; назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ, основные понятия и методы математической логики и теории алгоритмов диспетчеризации, способы проверки операционных систем на безопасность использования различных программных и аппаратных средств; основы администрирования вычислительных сетей; системы управления базами данных;
уметь: использовать программные и аппаратные средства персонального компьютера; определять предельные параметры информационных потоков, обрабатываемых вычислительным комплексом; моделировать операции по распределению ресурсов между процессами, формулировать и настраивать политику безопасности распространенных операционных построенных на их основе вычислительных сетей, систем, а также локальных вычислительных сетей, построенных на их основе, проверять операционные системы на безопасность использования различных программных и аппаратных средств; формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
владеть: навыками применения современных информационных технологий в профессиональной деятельности; методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов.

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

Производственная практика (эксплуатационная практика)

Производственная практика (преддипломная практика)

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-2: Способен администрировать средства защиты информации прикладного и системного программного обеспечения
ПК-2.7: Способен выявить естественнонаучную сущность проблем, возникающих в ходе профессиональной деятельности в области моделирования и анализа сложных естественных и искусственных систем
ПК-3: Способен устанавливать и настраивать средства защиты информации в автоматизированных системах
ПК-3.3: Знает основные меры по защите информации в автоматизированных системах
ПК-3.2: Владеет навыками установки и настройки средств защиты информации в автоматизированных системах
ПК-3.1: Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
ПК-4: Способен проводить работы по техническому обслуживанию защищенных технических средств защиты информации
ПК-4.3: Выполняет техническое обслуживание технических средств обработки информации в защищенном исполнении
ПК-4.2: Знает порядок аттестации объектов информатизации на соответствие требованиям безопасности информации
ПК-4.1: Знает проектную документацию на систему защиты объекта информатизации
ПК-5: Способен проводить мониторинг защищенности информации в автоматизированных системах
ПК-5.3: Анализирует недостатки в функционировании системы защиты информации автоматизированной системы
ПК-5.4: Применяет технические средства контроля эффективности средств защиты информации

ПК-5.1: Проводит мониторинг угроз безопасности информации в автоматизированных системах
ПК-5.2: Принимает меры защиты информации при выявлении новых угроз безопасности информации
ПК-6: Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах
ПК-6.1: Применяет руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
3.2	**Уметь:**
3.2.1	осуществлять меры противодействия нарушениям сетевой безопасности с испольованием различных программных и аппаратных средств защиты;
3.2.2	анализировать и оценивать угрозы информационной безопасности;
3.2.3	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проетирования, разработки и оценки защищенности компьютерных систем.
3.3	**Владеть:**
3.3.1	методами и средствами выявления угроз безопасности автоматизированным системам;
3.3.2	методами формирования требований по защите информации;
3.3.3	методами анализа и формализации информационных процессов объекта и связей между ними;
3.3.4	методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных докмуентов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Общие положения об информационной безопасности для телекоммуникационных систем					
1.1	Виды угроз информационной безопасности в телекоммуникационных системах /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.2	VPN как средство информационной безопасности /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.3	Варианты построения и средства защиты информации, дополняющие VPN /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.4	Состав программно-аппаратного комплекса ViPNet /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.5	Логическая структура сети ViPNet. Понятия адресной и прикладной администрации. Особенности ключевой структуры сети ViPNet /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
1.6	Практический семинар /Пр/	7	6	ПК-3.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	Работа в группе. Групповая дискуссия

1.7	Подготовка к практическому семинару /Ср/	7	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.8	Изучение литературы по тематике раздела /Ср/	7	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. ViPNet [Администратор] и его основные модули					
2.1	Ключевой и удостоверяющий центр ViPNet (УКЦ) /Лек/	7	2	ПК-3.2 ПК-3.3 ПК-4.1 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.2	Особенности взаимодействия ЦУС и УКЦ /Лек/	7	1	ПК-3.2 ПК-3.3 ПК-4.1 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.3	Состав файла-дистрибутива /Лек/	7	1	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
2.4	Подготовка к практическому семинару /Ср/	7	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
2.5	Практический семинар /Пр/	7	8	ПК-3.2 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	Работа в группе. Групповая дискуссия
2.6	Изучение литературы по тематике раздела /Ср/	7	6	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. ViPNet [Координатор] и его основные модули					
3.1	Функции ViPNet [Координатора]. Настройки координатора /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
3.2	Логика использования виртуальных адресов /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	

3.3	Практический семинар /Пр/	7	6	ПК-3.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	Работа в группе. Групповая дискуссия
3.4	Подготовка к практическому семинару /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
3.5	Изучение литературы по тематике раздела /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4	Л1.1Л2.1 Л2.2Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. ViPNet [Клиент] - характеристика и основные функции					
4.1	Персональный сетевой экран /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.2	Установление защищенных соединений /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.3	Услуги защищенных служб реального времени /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.4	Сервис защищенных почтовых услуг /Лек/	7	1	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2 Э1 Э2 Э3 Э4 Э5	
4.5	Практический семинар /Пр/	7	8	ПК-3.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	Работа в группе. Групповая дискуссия
4.6	Подготовка к практическому семинару /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
4.7	Изучение литературы по тематике раздела /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.2 Э1 Э2 Э3 Э4 Э5	
	Раздел 5. Типовые схемы применения технологии ViPNet					
5.1	Практический семинар /Пр/	7	8	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	Работа в группе. Групповая дискуссия

5.2	Подготовка к практическому семинару /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
5.3	Изучение литературы по тематике раздела /Ср/	7	8	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.2 Э1 Э2 Э3 Э4 Э5	
5.4	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	7	18	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
5.5	Промежуточная аттестация /Экзамен/	7	36	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э5	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине (модулю), состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине. Оценочные материалы размещаются 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	Зырянова Т. Ю.	Защита информационных процессов на транспорте: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Кузин А. В., Кузин Д.А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2020	http://znanium.com
Л2.2	Максимов Н. В., Попов И.И.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2021	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Защита информационных процессов на транспорте: методические рекомендации к практическим семинарам по дисциплине «Защита информационных процессов на транспорте» для студентов направления подготовки 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Зырянова Т. Ю.	Защита информационных процессов на транспорте: методические рекомендации по организации самостоятельной работы по дисциплине «Защита информационных процессов на транспорте» 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	Официальный сайт ОАО "ИнфоТеКС" (http://www.infotecs.ru)
Э2	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)
Э3	Официальный сайт ФСТЭК России (http://www.fstec.ru)
Э4	Официальный сайт ФСБ России (http://www.fsb.ru)
Э5	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	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	Справочно-правовая система Гарант
6.3.2.3	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.4	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
6.3.2.5	Международная реферативная база данных научных изданий Scopus
6.3.2.6	Международная реферативная база данных научных изданий eLIBRARY.RU
6.3.2.7	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.8	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	Специализированная мебель

контроля и промежуточной аттестации	
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
Компьютерный класс - Учебная аудитория для самостоятельной работы студентов	Специализированная мебель 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
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
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. 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).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)".

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.