ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

ФТД.02 Программно-аппаратная защита информации

рабочая программа дисциплины (модуля)

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

Учебный план 09.04.02_ИТм_2023.plx
09.04.02 Информационные системы и технологии

Направленность (профиль) Системное администрирование информационно-коммуникационных систем

Квалификация **магистр**

Форма обучения **очная**

Объем дисциплины (модуля) **2 ЗЕТ**

Часов по учебному плану 72
в том числе:
аудиторные занятия 36
самостоятельная работа 36

Часов контактной работы всего, в том числе: 37,8
аудиторная работа 36
текущие консультации по практическим занятиям 1,8

Промежуточная аттестация и формы контроля:
зачет 1

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**1 (1.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	18	18	18	18
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	36	36	36	36
Итого	72	72	72	72

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины:Подготовить выпускника к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники для организации защиты информации.
1.2	Задачи дисциплины: сформировать у обучающегося знания принципов и методов противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации и умения осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.

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

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в рамках образовательных программ (уровень бакалавриата или специалитета) в области информационных технологий.

В результате освоения предшествующих дисциплин обучающийся должен знать: место и роль информационной безопасности в системе национальной безопасности Российской Федерации; методы программирования и методы разработки эффективных алгоритмов решения прикладных задач; основы администрирования вычислительных сетей; назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ;
уметь: использовать программные и аппаратные средства персонального компьютера; анализировать и оценивать угрозы информационной безопасности объекта; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; 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; самостоятельно работать с учебной, справочной и учебно-методической литературой; 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;
владеть: методами и средствами выявления угроз безопасности автоматизированным системам; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов; навыками работы с учебной и учебно-методической литературой; методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации.

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

Производственная практика (преддипломная практика)Государственная итоговая аттестация

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-5: Способен разрабатывать и модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-5.2: Умеет модернизировать программное и аппаратное обеспечение информационных и автоматизированных систем для решения профессиональных задач
ОПК-5.1: Знает современное программное и аппаратное обеспечение информационных и автоматизированных систем
ОПК-2: Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач
ОПК-2.1: Знает современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач
ОПК-1: Способен самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте
ОПК-1.2: Умеет решать нестандартные профессиональные задачи, в том числе в новой или незнакомой среде и в междисциплинарном контексте, с применением математических, естественнонаучных, социально-экономических и профессиональных знаний
УК-2: Способен управлять проектом на всех этапах его жизненного цикла
УК-2.3: Разрабатывает план реализации проекта
УК-2.1: Формулирует цели, задачи, значимости, ожидаемые результаты проектов

УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий
УК-1.1: Анализирует проблемную ситуацию, выявляет ее составляющие, устанавливает связи
ПК-1.2: Способность осуществлять администрирование СУБД инфокоммуникационной системы организации
ПК-1.2.5: Знает способы и методы резервного копирования и восстановления баз данных
ПК-1.2.3: Имеет навык конфигурации средств разграничения доступа операционных систем и СУБД
ПК-1.3: Способность осуществлять администрирование системного программного обеспечения инфокоммуникационной системы организации
ПК-1.3.4: Имеет навык применения программных, программно-аппаратных средств защиты для разграничения доступа в инфокоммуникационной системе
ПК-1.3.2: Знает принципы информационной безопасности и защиты информации в инфокоммуникационных системах

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	аппаратные средства вычислительной техники; принципы построения информационных систем;
3.1.2	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 использованием различных программных и аппаратных средств защиты;
3.2.2	выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах.
3.3	**Владеть:**
3.3.1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений;
3.3.2	навыками выявления и уничтожения компьютерных вирусов;
3.3.3	методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Защита информации в автоматизированных системах					
1.1	Защита информации в автоматизированных системах /Лек/	1	4	УК-1.1 ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2	Л1.1 Э1 Э2 Э3 Э4	
1.2	Описание организационной и информационной структуры предприятия /Пр/	1	2	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2	Л1.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе, анализ практических структур предприятий
1.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	1	6	УК-1.1 ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Э1 Э4	
1.4	Подготовка отчета по практической работе /Ср/	1	4	УК-1.1 УК-2.3 ОПК-1.2 ОПК-5.2	Л1.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 2. Управление доступом в компьютерных системах					

2.1	Модели управления доступом в информационных системах и сетях /Лек/	1	4	УК-1.1 ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2	Л1.1	
2.2	Безопасность передачи информации через сеть /Лек/	1	2	УК-1.1 ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2	Л1.1	
2.3	Управление доступом в операционных системах. Идентификация и аутентификация пользователей операционных систем /Пр/	1	2	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2	Л1.1Л2.1Л3.1 Л3.2 Э1 Э4	Работа в группе, решение практико-ориентированных задач по освоению технологии
2.4	Изучение литературы и нормативных документов по тематике раздела /Ср/	1	4	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э4	
2.5	Идентификация и аутентификация пользователей информационных систем /Пр/	1	2	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.3.2 ПК-1.3.4	Л1.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группах, моделирование ситуации
2.6	Политики паролей в операционных системах /Пр/	1	2	ОПК-5.1 ОПК-5.2 ПК-1.3.4	Л1.1Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группах, отработка навыков
2.7	Внедрение в операционную систему программных систем защиты информации /Пр/	1	2	ОПК-2.1 ОПК-5.1 ПК-1.2.5 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группах, моделирование ситуации
2.8	Защита передачи информации с помощью систем виртуальных частных сетей /Пр/	1	2	ОПК-5.2 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группах, моделирование ситуации
2.9	Подготовка отчета по практическим работам /Ср/	1	4	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.2.5 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.1Л3.1 Э1 Э2 Э3 Э4	
	Раздел 3. Защита информации от разрушающего воздействия вредоносных программ					
3.1	Сети периметра и межсетевое экранирование /Лек/	1	4	ОПК-5.1 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.1Л3.1 Э1 Э2 Э3 Э4	
3.2	Антивирусные средства защиты /Пр/	1	4	ОПК-5.1 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	Работа в группе, освоение технологии
3.3	Подготовка отчета по практической работе /Ср/	1	2	ОПК-5.1 ПК-1.3.2 ПК-1.3.4	Л1.1Л2.1Л3.1 Э1 Э2 Э3 Э4	

3.4	Изучение основной литературы по курсу /Ср/	1	4	ОПК-5.1 ПК-1.3.2 ПК-1.3.4	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 Э4	
	Раздел 4. Защита современных операционных систем					
4.1	Управление доступом в операционных системах различных категорий /Лек/	1	4	ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.2.5 ПК-1.3.4	Л1.1 Э1 Э2 Э3 Э4	
4.2	Обзор систем управления безопасностью /Пр/	1	2	УК-1.1 ОПК-2.1 ОПК-5.1 ПК-1.2.3 ПК-1.2.5 ПК-1.3.2	Л1.1Л2.1Л3.1 Л3.2 Э2 Э3 Э4	Работа в группе, изучение практического применения изученных технологий
4.3	Изучение литературы и нормативных документов по тематике раздела, подготовка доклада с презентацией по теме /Ср/	1	4	УК-1.1 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.2.5 ПК-1.3.4	Л1.1Л3.1 Э1 Э2 Э3 Э4	
4.4	Подготовка отчетов по практическим работам /Ср/	1	2	УК-1.1 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.2.5 ПК-1.3.2 ПК-1.3.4	Л1.1Л3.1 Э1 Э2 Э3 Э4	
4.5	Подготовка к промежуточной аттестации /Ср/	1	6	УК-1.1 УК-2.1 УК-2.3 ОПК-1.2 ОПК-2.1 ОПК-5.1 ОПК-5.2 ПК-1.2.3 ПК-1.2.5 ПК-1.3.2 ПК-1.3.4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	

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	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.2	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО□, 2021	http://znanium.com

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Платонов В. В.	Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей: учебное пособие для студентов вузов, обучающихся по специальностям 090102 - "Компьютерная безопасность", 090105 - "Комплексное обеспечение информационной безопасности автоматизированных систем"	Москва: Академия, 2006	
Л2.2	Кусек К., Ван Ной В., Дэниел А.	Администрирование VMware vSphere 5: [пер. с англ.]	Санкт-Петербург: Питер, 2013	
Л2.3	Бабаш А.В.	Криптографические методы защиты информации: Учебно-методическое пособие: Том 1	Москва: Издательский Центр РИО□, 2021	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А.	Администрирование информационных систем: методические рекомендации к самостоятельной работе по дисциплине «Администрирование информационных систем» для студентов направления подготовки 09.03.02 - «Информационные системы и технологии»	Екатеринбург: УрГУПС, 2015	http://biblioserver.usurt.ru
Л3.2	Гузенкова Е. А., Паршина Е. В.	Администрирование информационных систем: методические рекомендации к практическим работам по дисциплине «Администрирование информационных систем» для студентов направления подготовки 09.03.02 «Информационные системы и технологии» всех форм обучения	Екатеринбург: УрГУПС, 2015	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Э1	www.knorus.ru — Сайт издательства КНОРУС
Э2	www.e-commerce.ru — Информационно-консалтинговый центр по электронному бизнесу
Э3	www.vadimeidlin.com — Сайт по электронной коммерции и web-маркетингу Вадима Ельнина
Э4	Среда электронного обучения BlackBoard Learn - bb.usurt.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
6.3.1.7	Secret Net Studio
6.3.1.8	Система защиты информации от несанкционированного доступа: Dallas Lock
6.3.1.9	Linux Debian

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	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.4	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 Программно-аппаратный комплекс "Соболь". Версия 4, PCIe, сертификат ФСТЭК России. Rutoken S 64КБ НДВ3, сертификат ФСТЭК России 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 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
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 текущего контроля и промежуточной аттестации	Специализированная мебель

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. Самостоятельная работа, связанная с оформлением отчетов по практическим занятиям организована таким образом, чтобы обучающиеся имели возможность получать обратную связь о результатах их выполнения по мере готовности до начала промежуточной аттестации. Для этого отчеты по практическим занятиям направляются в адрес преподавателя, который проверяет их и возвращает обучающемуся с комментариями. 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. Требования к объему и содержанию отчетов по практическим занятиям а также качеству их выполнения идентичны для обучающихся всех форм обучения.
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.