

**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**  
 Федеральное государственное бюджетное образовательное учреждение  
 высшего образования  
 "Уральский государственный университет путей сообщения"  
 (ФГБОУ ВО УрГУПС)

## **Б1.Б.Д.05 Технологии обеспечения информационной безопасности**

### **рабочая программа дисциплины (модуля)**

Закреплена за кафедрой	<b>Информационные технологии и защита информации</b>		
Учебный план	10.04.01_ИБм_2021.plx		
Направленность (профиль)	Направление подготовки 10.04.01 Информационная безопасность		
Квалификация	Информационная безопасность на транспорте		
Форма обучения	<b>магистр</b>		
Объем дисциплины (модуля)	<b>очная</b>		
Часов по учебному плану	<b>3 ЗЕТ</b>	Часов контактной работы всего, в том числе:	<b>40,3</b>
в том числе:	108	аудиторная работа	36
аудиторные занятия	36	текущие консультации по лабораторным занятиям	0,8
самостоятельная работа	36	текущие консультации по практическим занятиям	1
часов на контроль	36	консультации перед экзаменом	2
Промежуточная аттестация и формы контроля:		прием экзамена	0,5
экзамен	1		

**Распределение часов дисциплины по семестрам**

Семестр (<Курс>.<Семестр на курсе>)	1 (1.1)		Итого	
	18			
Неделя	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	8	8	8	8
Практические	10	10	10	10
Итого ауд.	36	36	36	36
Контактная работа	36	36	36	36
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	108	108	108	108

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: теоретическая и практическая подготовка специалистов к деятельности, связанной с разработкой и внедрением политики обеспечения комплексной безопасности объектов информатизации
1.2	Задачи дисциплины: изучение методологических подходов и принципов организации защиты информации; изучение методов проектирования технологий обеспечения информационной безопасности; изучение состава технического, программного и информационного обеспечения информационных систем

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	Б1.Б.Д
<b>2.1 Требования к предварительной подготовке обучающегося:</b>	
Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения соответствующих дисциплин по программе бакалавриата или специалитета. В результате освоения предшествующих дисциплин обучающийся должен: Знать: основные методы и средства обеспечения безопасности в системах управления базами данных; основные методы и средства обеспечения безопасности операционных систем; Уметь осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; Владеть навыками настройки подсистем защиты основных операционных систем.	
<b>2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>	
Производственная практика (проектно-технологическая практика) Управление информационной безопасностью Информационная безопасность объектов транспортной инфраструктуры Производственная практика (преддипломная практика) Государственная итоговая аттестация	

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
<b>УК-1: Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий</b>	
<b>УК-1.5: Выбирает способы обоснования решения проблемной ситуации</b>	
<b>УК-1.4: Вырабатывает стратегию решения поставленной задачи (составляет модель, определяет ограничения, вырабатывает критерии, оценивает необходимость дополнительной информации)</b>	
<b>УК-2: Способен управлять проектом на всех этапах его жизненного цикла</b>	
<b>УК-2.4: Осуществляет контроль реализации проекта</b>	
<b>УК-2.5: Оценивает эффективность реализации проекта и разрабатывает план действий по его корректировке</b>	
<b>УК-2.3: Разрабатывает план реализации проекта</b>	
<b>УК-2.1: Формулирует цели, задач, значимости, ожидаемые результаты проектов</b>	
<b>УК-2.2: Определяет потребности в ресурсах для реализации проекта</b>	
<b>ОПК-1: Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание</b>	
<b>ОПК-1.2: Разрабатывает проект технического задания на создание системы обеспечения информационной безопасности</b>	
<b>ОПК-2: Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности</b>	
<b>ОПК-2.2: Владеет технологией разработки технического проекта системы (подсистемы либо компонента системы) обеспечения информационной безопасности</b>	

В результате освоения дисциплины обучающийся должен

<b>3.1</b>	<b>Знать:</b>
3.1.1	методы концептуального проектирования технологий обеспечения информационной безопасности; принципы организации защиты информации; подходы к построению модели нарушителя и объекта с точки зрения информационной безопасности
<b>3.2</b>	<b>Уметь:</b>
3.2.1	осуществлять выбор функциональной структуры системы обеспечения информационной безопасности; обосновать принципы организации технического, программного и информационного обеспечения информационной безопасности; организовывать работы по совершенствованию, модернизации и унификации технологий обеспечения информационной безопасности
<b>3.3</b>	<b>Владеть:</b>

3.3.1	навыками работы с нормативными правовыми актами; навыками работы с нормативными документами; методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; методами организации и управления деятельностью служб защиты информации на предприятии; 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
	<b>Раздел 1. Подсистемы обеспечения безопасности объекта информатизации</b>					
1.1	Понятие и сущность защиты информации. Теоретические основы защиты информации. Состав и основные свойства защищаемой информации /Лек/	1	6	УК-1.4 УК-1.5	Л1.1Л2.1 Э1 Э2 Э3 Э5	
1.2	Каналы утечки информации и методы несанкционированного доступа к конфиденциальной информации. Объекты защиты информации /Лек/	1	4	УК-1.4 УК-1.5	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5	
1.3	Классификация видов, методов и способов защиты информации. Назначение и структура систем защиты информации /Лек/	1	4	УК-1.4 УК-1.5	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э4 Э5	
1.4	Подсистемы комплексной системы защиты информации /Пр/	1	10	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л1.2Л2.1Л3.2 Э1 Э2 Э3 Э4 Э5	Работа в группе, анализ подсистем комплексной системы защиты информации
1.5	Изучение основной и дополнительной литературы. Подготовка к семинарским занятиям /Ср/	1	12	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л1.1 Л1.2Л2.1Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	<b>Раздел 2. Комплексный подход к обеспечению безопасности объектов информатизации</b>					
2.1	Комплексная система защиты информации на предприятии /Лек/	1	4	УК-1.4 УК-1.5	Л1.1 Л1.2Л2.1 Э1 Э2 Э3 Э5	
2.2	Сущность и понятие информационной безопасности, характеристика ее составляющих. Значение информационной безопасности для субъектов информационных отношений /Лаб/	1	2	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л2.1Л3.1 Э1 Э2 Э3 Э5	Работа в малых группах, анализ составляющих информационной безопасности субъектов информационных отношений
2.3	Понятие и сущность защиты информации. Защищаемая информация – основные свойства и состав. Место защиты информации в системе информационной безопасности Российской Федерации. Классификация информации ограниченного доступа /Лаб/	1	2	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л2.1Л3.1 Э1 Э2 Э3 Э5	Работа в малых группах, анализ защищаемой информации

2.4	План защиты информации на предприятии /Лаб/	1	2	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л2.1Л3.1 Э1 Э2 Э3 Э5	Работа в малых группах, составление плана защиты информации на предприятии
2.5	Методологические подходы к защите информации и принципы ее организации. Объекты защиты. Виды защиты. Классификация методов и средств защиты информации /Лаб/	1	2	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л2.1Л3.1 Э1 Э2 Э3 Э5	Работа в малых группах, анализ методов и средств защиты информации
2.6	Подготовка к лабораторным занятиям /Ср/	1	12	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
2.7	Изучение основной и дополнительной литературы. Подготовка к промежуточной аттестации /Ср/	1	12	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л1.2Л2.1Л3.1 Л3.3 Э1 Э2 Э3 Э5	
2.8	Промежуточная аттестация /Экзамен/	1	36	УК-1.4 УК-1.5 УК-2.1 УК-2.2 УК-2.3 УК-2.4 УК-2.5 ОПК-1.2 ОПК-2.2	Л1.1 Л1.2Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	

### 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	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: конспект лекций для студентов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
Л1.2	Паршин К. А.	Оценка уровня информационной безопасности на объекте информатизации: допущено Федеральным агентством железнодорожного транспорта в качестве учебного пособия для студентов вузов железнодорожного транспорта	Москва: ФГБОУ "Учеб.-метод. центр по образованию на ж.-д. трансп.", 2015	<a href="https://umczdt.ru/books/">https://umczdt.ru/books/</a>

##### 6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Куприянов А. И., Сахаров А. В., Шевцов В. А.	Основы защиты информации: учебное пособие для студентов, обучающихся по специальностям "Радиоэлектронные системы", "Средства радиоэлектронной борьбы", "Информационные системы и технологии"	Москва: Академия, 2007	

### 6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: методические рекомендации к лабораторным занятиям для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
Л3.2	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: методические рекомендации к практическим семинарам по дисциплине «Технологии обеспечения информационной безопасности объектов» для студентов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>
Л3.3	Зырянова Т. Ю.	Технологии обеспечения информационной безопасности объектов: методические рекомендации по организации самостоятельной работы студентов по дисциплине «Технологии обеспечения информационной безопасности объектов» для студентов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	<a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a>

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

Э1	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) ( <a href="http://iso27000.ru">http://iso27000.ru</a> )
Э2	Информационный бюллетень компании "Инфосистемы Джет" ( <a href="http://www.jetinfo.ru">http://www.jetinfo.ru</a> )
Э3	Система электронной поддержки обучения BlackBoard Learn ( <a href="http://bb.usurt.ru">http://bb.usurt.ru</a> )
Э4	Официальный сайт ФСТЭК России ( <a href="http://www.fstec.ru">http://www.fstec.ru</a> )
Э5	Официальный сайт ФСБ России ( <a href="http://www.fsb.ru">http://www.fsb.ru</a> )

### 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	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	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
6.3.2.3	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.4	Банк данных угроз безопасности информации ФСТЭК России: <a href="https://bdu.fstec.ru/">https://bdu.fstec.ru/</a>
6.3.2.5	Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00
6.3.2.6	ЭБС УМЦ ЖДТ по адресу <a href="https://umczdt.ru/books/">https://umczdt.ru/books/</a>
6.3.2.7	ЭБС IPR SMART по адресу <a href="http://www.iprbookshop.ru/586.html">http://www.iprbookshop.ru/586.html</a>
6.3.2.8	Электронная библиотека диссертаций Российской государственной библиотеки по адресу <a href="https://dvs.rsl.ru/">https://dvs.rsl.ru/</a>

## 7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯ БАЗА, НЕОБХОДИМАЯ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Назначение	Оснащение
------------	-----------

<p>Лаборатория «Технологии обеспечения информационной безопасности и техническая защита информации». 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.</p>	<p>Специализированная мебель Лабораторное оборудование: Анализатор качества электроэнергии в трехфазных сетях FLUKE 435 Анализатор спектра портативный R&amp;S FSH 4/8 Комплекс программно-аппаратный Oscor-5000 Всенаправленный источник звука Brüel&amp;Kjær 4296 Генератор шума "ГРОМ-ЗИ-4" Детектор звукозаписывающих устройств Имитатор электростатических разрядов ЭСР-8000 К Индикатор поля D-008 Подавитель сотовой связи ЛПС-718 Тестер кабельный MicroScanner2 Универсальный анализатор проводных линий ULAN-2 Шумомер-вибромметр, анализатор спектра портативный ОКТАВА-110А с антеннами измерительными Система автоматизированная измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов СТЕНТОР-М1 Комплекс для проведения акустических и виброакустических измерений "Спрут-7А" Оборудование для центра защиты информации, включающее комплекс виброакустической защиты "Барон", поисковый прибор "ОРИОН", измеритель параметров проводных коммуникаций LBD-50, прибор блокирования сотовых телефонов "Скат" Многофункциональный поисковый прибор SPYDER Ручной селективный металлодетектор EH-MD1 Селективный индикатор поля RAKSA-120 Портативный измеритель частоты и мощности РИЧ-8 (MFP-8000) Обнаружитель скрытых видеокamer по оптическому признаку с лазерной подсветкой Прометей Устройство для защиты линий электропитания и заземления от утечки информации. Средство активной защиты информации от утечки за счет ПЭМИН Соната-Р3 Устройство блокирования работы систем цифровой связи и передачи данных Квартет-2 Подавитель диктофонов и микрофонов Бубен-Ультра Генератор звуковой акустической помехи Бубен Система активной защиты информации от утечки за счет ПЭМИН SEL SP-44 Однофазный сетевой помехоподавляющий фильтр ЛППФ-10-1Ф Устройство защиты громкоговорителя МП-5 Тестер блокираторов сотовой связи и беспроводной передачи данных</p>
<p>Учебная аудитория для проведения текущего контроля и промежуточной аттестации</p>	<p>Специализированная мебель</p>
<p>Учебная аудитория для проведения занятий лекционного типа</p>	<p>Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы</p>
<p>Компьютерный класс - Учебная аудитория для самостоятельной работы студентов</p>	<p>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</p>
<p>Учебная аудитория для проведения групповых и индивидуальных консультаций</p>	<p>Специализированная мебель</p>
<p>Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации</p>	<p>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</p>
<p>Лаборатория "Сети и системы передачи информации". Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных</p>	<p>Специализированная мебель Лабораторное оборудование: Анализатор спектра GSP-810 Генератор сигналов AFG3101 Источник питания регулируемый MASTECH NY3020 Осциллограф цифровой GDS-820C Осциллограф цифровой GDS-71102A Телефоны Cisco IP Антенна параболическая офсетная с кронштейном Супрал СТВ 1.2-1.1 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</p>

консультаций, текущего контроля и промежуточной аттестации.	Технические средства обучения - Комплект мультимедийного оборудования
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, а также для самостоятельной работы. Специализированный кабинет «Управление информационной безопасностью».	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 Технические средства обучения - Комплект мультимедийного оборудования
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
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
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

## **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](http://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](http://bb.usurt.ru)) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Самостоятельная работа организована таким образом, чтобы обучающиеся имели возможность получать обратную связь о ее результатах до начала промежуточной аттестации. Совместная деятельность преподавателя и обучающихся организована в системе электронной поддержки обучения Blackboard Learn (сайт [bb.usurt.ru](http://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](http://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](http://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](http://bb.usurt.ru))) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений