**ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА**

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

# Б1.Б.19 Основы управления информационной безопасностью

## 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) **4 ЗЕТ**

| | | | |
|---|---|---|---|
| Часов по учебному плану | 144 | Часов контактной работы всего, в том числе: | 40,3 |
| в том числе: | | аудиторная работа | 36 |
| аудиторные занятия | 36 | текущие консультации по практическим занятиям | 1,8 |
| самостоятельная работа | 72 | консультации перед экзаменом | 2 |
| часов на контроль | 36 | прием экзамена | 0,5 |

Промежуточная аттестация и формы контроля:
экзамен 7

**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 | 18 | 18 | 18 | 18 |
| Итого ауд. | 36 | 36 | 36 | 36 |
| Контактная работа | 36 | 36 | 36 | 36 |
| Сам. работа | 72 | 72 | 72 | 72 |
| Часы на контроль | 36 | 36 | 36 | 36 |
| Итого | 144 | 144 | 144 | 144 |

| 1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ) | |
|---|---|
| 1.1 | Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии. |
| 1.2 | Приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации в управлении информационной безопасностью. |
| 1.3 | Формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности. |

| 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 дисциплины Теория информационной безопасности и методология защиты информации.
В результате освоения предшествующих дисциплин обучающийся должен знать: основы российской правовой системы и законодательства; основные понятия и методы в управленческой деятельности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; методологию создания систем защиты информации;
уметь: использовать в практической деятельности правовые знания; оценивать эффективность управленческих решений; анализировать и оценивать угрозы информационной безопасности объекта; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и модели нарушителей информационной безопасности выявлять уязвимости информационных ресурсов, проводить мониторинг угроз информационной безопасности;
владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками обоснования, выбора, реализации и контроля результатов управленческого решения; профессиональными способами обеспечения безопасности в сфере информации; профессиональной терминологией в области информационной безопасности.

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

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 ресурсов, подлежащих защите |
| Уровень 2 | классификацию угроз информационной безопасности и возможные пути их реализации |
| Уровень 3 | методы анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| **Уметь:** | |
| Уровень 1 | определять защищаемую информацию |
| Уровень 2 | определять угрозы защищаемой информации |
| Уровень 3 | - |
| **Владеть:** | |
| Уровень 1 | навыками анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты |
| Уровень 2 | - |
| Уровень 3 | - |

| **ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты** | |
|---|---|
| **Знать:** | |
| Уровень 1 | цели, задачи, принципы и основные направления обеспечения информационной безопасности |
| Уровень 2 | принципы организации информационных систем в соответствии с требованиями по защите информации |
| Уровень 3 | принципы формирования политики информационной безопасности в информационных системах |
| **Уметь:** | |
| Уровень 1 | выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов защиты информации |

| | |
|---|---|
| Уровень 2 | оценивать комплекс мер по информационной безопасности на основании выбранных критериев |
| Уровень 3 | контролировать эффективность принятых мер по защите информации |
| **Владеть:** | |
| Уровень 1 | навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем |
| Уровень 2 | навыками организации информационных систем в соответствии с требованиями по защите информации |
| Уровень 3 | навыками участия в экспертизе состояния защищенности информации на объекте защиты |

| **ПСК-2: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия** | |
|---|---|
| **Знать:** | |
| Уровень 1 | основные методы управления информационной безопасностью |
| Уровень 2 | основные угрозы безопасности информации и модели нарушителя в информационных системах |
| Уровень 3 | принципы формирования политики информационной безопасности в информационных системах |
| **Уметь:** | |
| Уровень 1 | выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем |
| Уровень 2 | определять комплекс мер для обеспечения информационной безопасности информационных систем |
| Уровень 3 | контролировать эффективность принятых мер по обеспечению информационной безопасности |
| **Владеть:** | |
| Уровень 1 | навыками анализа информационной инфраструктуры информационных систем и ее безопасности; методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем |
| Уровень 2 | навыками выбора и обоснования критериев эффектиности функционирования защищенных информационных систем |
| Уровень 3 | навыками участия в экспертизе состояния защищенных информационных систем |

| **ПСК-3: способностью участвовать в разработке подсистемы управления информационной безопасностью** | |
|---|---|
| **Знать:** | |
| Уровень 1 | основные методы управления информационной безопасностью |
| Уровень 2 | основные угрозы безопасности информации и модели нарушителя в информационных системах |
| Уровень 3 | принципы формирования политики информационной безопасности |
| **Уметь:** | |
| Уровень 1 | определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите |
| Уровень 2 | разрабатывать модели угроз и нарушителей информационной безопасности информационных систем |
| Уровень 3 | разрабатывать политики безопасности информационных систем |
| **Владеть:** | |
| Уровень 1 | навыками анализа информационной инфраструктуры информационной системы и ее безопасности |
| Уровень 2 | методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем |
| Уровень 3 | навыками участия в экспертизе состояния защищенности информации на объекте защиты |

| **ПСК-5: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью** | |
|---|---|
| **Знать:** | |
| Уровень 1 | методологию создания систем защиты информации |
| Уровень 2 | современные подходы к построению систем защиты информации |
| Уровень 3 | перспективные направления развития средств и методов защиты информации |
| **Уметь:** | |
| Уровень 1 | пользоваться современной научно-технической информацией по исследуемым задачам |
| Уровень 2 | применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности |
| Уровень 3 | разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации |
| **Владеть:** | |
| Уровень 1 | навыками анализа информационной инфраструктуры информационной системы и ее безопасности |
| Уровень 2 | методами формирования требований по защите информации |
| Уровень 3 | методами мониторинга и аудита, выявления угроз информационной безопасности |

| ПСК-6: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью | |
|---|---|
| **Знать:** | |
| Уровень 1 | основные методы управления информационной безопасностью |
| Уровень 2 | основные угрозы безопасности информации и модели нарушителя в информационных системах |
| Уровень 3 | принципы формирования политики информационной безопасности в информационных системах |
| **Уметь:** | |
| Уровень 1 | определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите |
| Уровень 2 | разрабатывать модели угроз и модели нарушителей информационной безопасности информационных систем |
| Уровень 3 | определять комплекс мер для обеспечения информационной безопасности информационных систем |
| **Владеть:** | |
| Уровень 1 | навыками анализа информационной инфраструктуры информационной системы и ее безопасности |
| Уровень 2 | методами мониторинга и аудита, выявления угроз информационной безопасности |
| Уровень 3 | навыками выбора комплекса мер для обеспечения информационной безопасности информационных систем |

**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; |
| 3.1.2 | принципы организации информационных систем в соответствии с требованиями по защите информации; |
| 3.1.3 | основные нормативные правовые акты в области информационной безопасности и защиты информации. |
| **3.2** | **Уметь:** |
| 3.2.1 | анализировать и оценивать угрозы информационной безопасности объекта; |
| 3.2.2 | применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; |
| 3.2.3 | пользоваться нормативными документами по защите информации; |
| 3.2.4 | формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе. |
| **3.3** | **Владеть:** |
| 3.3.1 | навыками работы с нормативными правовыми актами; |
| 3.3.2 | навыками работы с нормативными документами; |
| 3.3.3 | методами и средствами выявления угроз безопасности автоматизированным системам; |
| 3.3.4 | методами формирования требований по защите информации; |
| 3.3.5 | методами анализа и формализации информационных процессов объекта и связей между ними; |
| 3.3.6 | методами организации и управления деятельностью служб защиты информации на предприятии; |
| 3.3.7 | 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. Введение в системы управления информационной безопасностью** | | | | | |
| 1.1 | Основные понятия и определения /Лек/ | 7 | 2 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |
| 1.2 | Система управления информационной безопасностью /Лек/ | 7 | 2 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |
| 1.3 | Политика безопасности /Лек/ | 7 | 2 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| 1.4 | Организация обеспечения информационной безопасности информационных систем /Лек/ | 7 | 4 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |
| 1.5 | Аудит информационной безопасности /Лек/ | 7 | 4 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |
| 1.6 | Средства поддержки процессов управления информационной безопасностью /Лек/ | 7 | 4 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 | Л1.1Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 | |
| 1.7 | Изучение нормативных документов по тематике дисциплины /Ср/ | 7 | 36 | ПСК-6 | Л1.1 Э1 Э4 | |
| | **Раздел 2. Управление информационной безопасностью в информационных системах персональных данных** | | | | | |
| 2.1 | Проектирование системы защиты персональных данных /Пр/ | 7 | 18 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 ОПК-7 | Л1.1Л2.1 Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 | Работа в группе, решение практико-ориентированных задач |
| 2.2 | Подготовка отчета по практическому разделу /Ср/ | 7 | 36 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 ОПК-7 | Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 | |
| 2.3 | Промежуточная аттестация /Экзамен/ | 7 | 36 | ПК-4 ПСК-2 ПСК-3 ПСК-5 ПСК-6 ОПК-7 | Л1.1Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 | |

## 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 | Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И. | Основы управления информационной безопасностью: допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по программам бакалавриата, магистратуры и специалитета укрупненного направления 090000 - "Информационная безопасность" | Москва: Горячая линия - Телеком, 2012 | http://e.lanbook.com |

#### 6.1.2. Дополнительная учебная литература

| | Авторы, составители | Заглавие | Издательство, год | Web-ссылка |
|---|---|---|---|---|

| | Авторы, составители | Заглавие | Издательство, год | Web-ссылка |
|---|---|---|---|---|
| Л2.1 | Грибунин В. Г., Чудовский В. В. | Комплексная система защиты информации на предприятии: учебное пособие для студентов вузов, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации" | Москва: Академия, 2009 | |
| Л2.2 | Мельников В. П., Клейменов С. А., Петраков А. М., Клейменов С. А. | Информационная безопасность и защита информации: учебное пособие для студентов вузов, обучающихся по специальности 230201 - "Информационные системы и технологии" | Москва: Академия, 2009 | |
| Л2.3 | Шаньгин В. Ф. | Комплексная защита информации в корпоративных системах: Учебное пособие | Москва: Издательский Дом "ФОРУМ", 2017 | http://znanium.com |

**6.1.3. Методические разработки**

| | Авторы, составители | Заглавие | Издательство, год | Web-ссылка |
|---|---|---|---|---|
| Л3.1 | Зырянова Т. Ю. | Основы управления информационной безопасностью: методические рекомендации по организации самостоятельной работы студентов по дисциплине «Основы управления информационной безопасностью» для 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 | Зырянова Т. Ю., Симонович В. Г. | Основы управления информационной безопасностью: методические рекомендации к практическим занятиям по дисциплине «Основы управления информационной безопасностью» для 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 |

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

| | |
|---|---|
| Э1 | Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru) |
| Э2 | Информационный бюллетень компании "Инфосистемы Джет" (http://www.jetinfo.ru) |
| Э3 | Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru) |
| Э4 | 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 | 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 | Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/ |
| 6.3.2.5 | Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 |
| 6.3.2.6 | ГОСТ Эксперт - единая база ГОСТов Российской Федерации |

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

| Назначение | Оснащение |
|---|---|
| Кабинет "Управление информационной безопасностью". | Специализированная мебель<br>Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в |

| | |
|---|---|
| Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий | электронную информационно-образовательную среду Университета<br>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<br>Демонстрационное оборудование - Комплект мультимедийного оборудования<br>Учебно-наглядные пособия - презентационные материалы |
| Компьютерный класс - Учебная аудитория для самостоятельной работы студентов | Специализированная мебель<br>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 |
| Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации | Специализированная мебель<br>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<br>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<br>Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета<br>Технические средства обучения - Комплект мультимедийного оборудования |
| Читальный зал Информационно-библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы | Специализированная мебель<br>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).