

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

## Б1.Б.Д.04 Защищенные информационные системы 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 |   |       |
| <b>Квалификация</b>                        | <b>магистр</b>  |   |       |
| Форма обучения                             | <b>очная</b>  |   |       |
| Объем дисциплины (модуля)                  | <b>3 ЗЕТ</b>  |   |       |
| Часов по учебному плану                    | 108   | Часов контактной работы всего, в том числе:   | 38,05 |
| в том числе:                               |   | аудиторная работа                             | 36    |
| аудиторные занятия                         | 36  | текущие консультации по лабораторным занятиям | 0,8   |
| самостоятельная работа                     | 36  | текущие консультации по практическим занятиям | 1     |
| Промежуточная аттестация и формы контроля: |   | прием зачета с оценкой                        | 0,25  |
| зачет с оценкой 1                          |   |   |       |

**Распределение часов дисциплины по семестрам**

| Семестр<br>(<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  |
| Элект                                  | 36      | 36  | 36    | 36  |
| Итого ауд.                             | 36      | 36  | 36    | 36  |
| Контактная работа                      | 72      | 72  | 72    | 72  |
| Сам. работа                            | 36      | 36  | 36    | 36  |
| Итого                                  | 108     | 108 | 108   | 108 |

## 1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

|     |  |
|-----|--|
| 1.1 | Цель дисциплины: изучение технологий, методов и средств создания защищенных информационных систем  |
| 1.2 | Задачи дисциплины: формирование у обучающихся навыков системного анализа прикладной области, выявления угроз и оценки уязвимостей информационных систем, разработки требований и критериев оценки защищенности информации. |

## 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 дисциплин по программе бакалавриата или специалитета.<br>В результате освоения предшествующих дисциплин обучающийся должен:<br>Знать принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации;<br>Уметь анализировать и оценивать угрозы информационной безопасности объекта; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; пользоваться нормативными документами по защите информации; формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе;<br>Владеть 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. |        |
| <b>2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:</b>  |        |
| Производственная практика (проектно-технологическая практика)<br>Управление информационной безопасностью<br>Информационная безопасность объектов транспортной инфраструктуры<br>Производственная практика (преддипломная практика)<br>Государственная итоговая аттестация   |        |

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

|  |
|--|
| <b>ОПК-1:</b> Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание                          |
| <b>ОПК-1.5:</b> Знает руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации   |
| <b>ОПК-1.4:</b> Знает национальные, межгосударственные и международные стандарты в области защиты информации   |
| <b>ОПК-1.1:</b> Знает и определяет требования к системе обеспечения информационной безопасности, методы и принципы управления процессом создания системы информационной безопасности |
| <b>ОПК-2:</b> Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности   |
| <b>ОПК-2.1:</b> Знает методы, принципы и этапы разработки технического проекта (подсистемы либо компонента системы) обеспечения информационной безопасности                          |

В результате освоения дисциплины обучающийся должен

|                     |   |
|---------------------|---|
| <b>3.1 Знать:</b>   |   |
| 3.1.1               | основные принципы организации технического, программного и информационного обеспечения защищенных информационных систем |
| <b>3.2 Уметь:</b>   |   |
| 3.2.1               | анализировать техническую и эксплуатационную документацию на системы и средства обеспечения информационной безопасности |
| <b>3.3 Владеть:</b> |   |
| 3.3.1               | устанавливать и настраивать средства и системы защиты информации;   |
| 3.3.2               | осуществлять сопровождение и администрирование защищенных информационных систем   |

## 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. Теоретические основы защищенных информационных систем</b>   |   |   |                               |   |  |
| 1.1 | Защищенные информационные системы и требования к ним /Лек/   | 1 | 2 | ОПК-1.1<br>ОПК-1.5<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 1.2 | Объекты защиты. Факторы, воздействующие на информацию. Угрозы /Лек/  | 1 | 2 | ОПК-1.1<br>ОПК-1.5<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 1.3 | Изучение основной и дополнительной литературы по тематике раздела /Ср/   | 1 | 6 | ОПК-1.1<br>ОПК-1.5<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3<br>Л2.5Л3.1<br>Э1 Э2 Э3 Э7 |  |
|     | <b>Раздел 2. Проектирование защищенных информационных систем</b>   |   |   |                               |   |  |
| 2.1 | Требования государственных стандартов, руководящих документов Гостехкомиссии России к защищенным информационным системам /Лек/ | 1 | 2 | ОПК-1.1<br>ОПК-1.4            | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 2.2 | Жизненный цикл и порядок создания автоматизированных систем /Лек/  | 1 | 2 | ОПК-1.1<br>ОПК-1.4<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 2.3 | Порядок создания изделий информационных технологий, удовлетворяющих требованиям безопасности /Лек/                             | 1 | 2 | ОПК-1.1<br>ОПК-1.4<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 2.4 | Проектирование автоматизированных систем /Лек/   | 1 | 2 | ОПК-1.1<br>ОПК-1.4<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э6<br>Э7  |  |
| 2.5 | Управление проектированием защищенных автоматизированных систем /Лек/  | 1 | 2 | ОПК-1.1<br>ОПК-1.4<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3 Л2.5<br>Э1 Э2 Э3 Э7        |  |
| 2.6 | Изучение основной и дополнительной литературы по тематике раздела /Ср/   | 1 | 6 | ОПК-1.1<br>ОПК-1.4<br>ОПК-2.1 | Л1.1<br>Л1.2Л2.2<br>Л2.3<br>Л2.5Л3.1<br>Э1 Э2 Э3 Э7 |  |
|     | <b>Раздел 3. Установка и сопровождение функционирования средств защиты информации в защищенных информационных системах</b>     |   |   |                               |   |  |
| 3.1 | Особенности использования специализированного прикладного программного обеспечения защищенных информационных систем /Лек/      | 1 | 2 | ОПК-1.1<br>ОПК-2.1            | Л1.3Л2.1<br>Л2.2<br>Л2.4Л3.3<br>Э3 Э4 Э7            |  |
| 3.2 | Настройка и применение системы защиты информации Secret Net Studio /Лаб/   | 1 | 4 | ОПК-1.1<br>ОПК-2.1            | Л1.3Л2.1<br>Л2.2<br>Л2.4Л3.3<br>Э3 Э4 Э7            | Работа в малых группах, анализ и применение прикладного программного обеспечения |

|  |  |   |    |  |  |   |
|--|--|---|----|--|--|---|
| 3.3  | Настройка и применение средства защиты информации от несанкционированного доступа Dallas Lock /Лаб/  | 1 | 4  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.1<br>Л2.2<br>Л2.4Л3.3<br>Э3 Э5 Э7   | Работа в малых группах, анализ и применени прикладного программного обеспечения |
| 3.4  | Изучение основной и дополнительной литературы по тематике раздела /Ср/   | 1 | 6  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.2<br>Л2.4Л3.1<br>Л3.3<br>Э3 Э4 Э5 Э7  |   |
| <b>Раздел 4. Применение защитных механизмов операционных систем на базе ядра Linux</b> |  |   |    |  |  |   |
| 4.1  | Особенности построения и применения операционных систем на базе ядра Linux /Лек/   | 1 | 2  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.3Л3.2<br>Э3 Э6  |   |
| 4.2  | Исследование файловых объектов с правами пользователя /Пр/   | 1 | 2  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.3Л3.2<br>Э3 Э6  | Работа в группах, анализ и применение системного программного обеспечения       |
| 4.3  | Исследование процессов в ОС Linux /Пр/   | 1 | 2  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.3Л3.2<br>Э3 Э6  | Работа в группах, анализ и применение системного программного обеспечения       |
| 4.4  | Монтирование файловых систем /Пр/  | 1 | 2  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.3Л3.2<br>Э3 Э6  | Работа в группах, анализ и применение системного программного обеспечения       |
| 4.5  | Исследование сетевых возможностей ОС Linux /Пр/  | 1 | 4  | ОПК-1.1<br>ОПК-2.1                       | Л1.3Л2.3Л3.2<br>Э3 Э6  | Работа в группах, анализ и применение системного программного обеспечения       |
| 4.6  | Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов по практическим и лабораторным занятиям /Элект/ | 1 | 36 | ОПК-1.1<br>ОПК-1.4<br>ОПК-1.5<br>ОПК-2.1 | Л1.1 Л1.2<br>Л1.3Л2.1<br>Л2.2 Л2.3<br>Л2.4<br>Л2.5Л3.1<br>Л3.2 Л3.3<br>Э1 Э2 Э3 Э4<br>Э5 Э6 Э7 |   |
| 4.7  | Подготовка к промежуточной аттестации /Ср/   | 1 | 18 | ОПК-1.1<br>ОПК-1.4<br>ОПК-1.5<br>ОПК-2.1 | Л1.1 Л1.2<br>Л1.3Л2.1<br>Л2.2 Л2.3<br>Л2.4<br>Л2.5Л3.1<br>Л3.2 Л3.3<br>Э1 Э2 Э3 Э4<br>Э5 Э6 Э7 |   |

### 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)

| <b>6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)</b> |   |  |  |   |
|--|---|--|--|---|
| <b>6.1.1. Основная учебная литература</b>  |   |  |  |   |
|  | Авторы, составители   | Заглавие   | Издательство, год  | Web-ссылка  |
| Л1.1   | Зырянова Т. Ю.  | Защищенные информационные системы: конспект лекций для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность»  | Екатеринбург: УрГУПС, 2016                                       | <a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a> |
| Л1.2   | Шаньгин В.Ф.  | Комплексная защита информации в корпоративных системах: Учебное пособие  | Москва: Издательский Дом "ФОРУМ", 2020                           | <a href="http://znanium.com">http://znanium.com</a>                     |
| Л1.3   | Хорев П. Б.   | Программно-аппаратная защита информации: Учебное пособие   | Москва: ООО "Научно-издательский центр ИНФРА-М", 2021            | <a href="http://znanium.com">http://znanium.com</a>                     |
| <b>6.1.2. Дополнительная учебная литература</b>  |   |  |  |   |
|  | Авторы, составители   | Заглавие   | Издательство, год  | Web-ссылка  |
| Л2.1   | Хорев П. Б.   | Методы и средства защиты информации в компьютерных системах: учебное пособие для студентов вузов, обучающихся по направлению 230100 - "Информатика и вычислительная техника"   | Москва: Академия, 2008   |   |
| Л2.2   | Гузенкова Е. А., Агафонов А. В., Мезенцев А. В., Синадский Н. И., Хорьков Д. А. | Технологии межсетевого экранирования и защищенной обработки информации: учебное пособие по дисциплине «Защищенные информационные системы» 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> |
| Л2.3   | Духан Е. И., Зырянова Т. Ю., Синадский Н. И.                                    | Средства защиты информации: учебное пособие по дисциплине "Защищенные информационные системы" для студентов 1 курса направления подготовки 10.04.01 - "Информационная безопасность"  | Екатеринбург: УрГУПС, 2016                                       | <a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a> |
| Л2.4   | Душкин А. В., Кольцов А.  | Аппаратные и программные средства защиты информации: Учебное пособие   | Воронеж: Издательско-полиграфический центр "Научная книга", 2016 | <a href="http://znanium.com">http://znanium.com</a>                     |
| Л2.5   | Баранова Е.К., Бабаш А.В.   | Информационная безопасность и защита информации: Учебное пособие   | Москва: Издательский Центр РИО□, 2021                            | <a href="http://znanium.com">http://znanium.com</a>                     |
| <b>6.1.3. Методические разработки</b>  |   |  |  |   |
|  | Авторы, составители   | Заглавие   | Издательство, год  | Web-ссылка  |
| Л3.1   | Зырянова Т. Ю.  | Защищенные информационные системы: методические рекомендации по организации самостоятельной работы по дисциплине «Защищенные информационные системы» для магистрантов направления подготовки 10.04.01 «Информационная безопасность» очной формы обучения | Екатеринбург: УрГУПС, 2016                                       | <a href="http://biblioserver.usurt.ru">http://biblioserver.usurt.ru</a> |
| Л3.2   | Зырянова Т. Ю.  | Защищенные информационные системы: методические рекомендации к практическим 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> |

|  | Авторы, составители   | Заглавие  | Издательство,<br>год       | Web-ссылка                   |
|--|---|---|----------------------------|------------------------------|
| Л3.3   | Зырянова Т. Ю.  | Защищенные информационные системы: методические рекомендации к лабораторным занятиям для студентов направления подготовки магистратуры 10.04.01 «Информационная безопасность» | Екатеринбург: УрГУПС, 2016 | http://biblioserver.usurt.ru |
| <b>6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)</b>   |   |   |                            |                              |
| Э1   | Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) по стандартам в области информационной безопасности (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 компании Код Безопасности (https://www.securitycode.ru)  |   |                            |                              |
| Э5   | Официальный сайт компании Конфидент (http://www.confident.ru/)  |   |                            |                              |
| Э6   | Сайт поддержки разработчиков и пользователей операционной системы Linux Debian (https://www.debian.org/)                    |   |                            |                              |
| Э7   | Официальный сайт ФСТЭК России (http://www.fstec.ru)   |   |                            |                              |
| <b>6.3 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем</b> |   |   |                            |                              |
| <b>6.3.1 Перечень программного обеспечения</b>   |   |   |                            |                              |
| 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   |   |                            |                              |
| 6.3.1.5  | Linux Debian  |   |                            |                              |
| 6.3.1.6  | Secret Net Studio   |   |                            |                              |
| 6.3.1.7  | Система защиты информации от несанкционированного доступа: Dallas Lock  |   |                            |                              |
| <b>6.3.2 Перечень информационных справочных систем и профессиональных баз данных</b>   |   |   |                            |                              |
| 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: https://bdu.fstec.ru/   |   |                            |                              |
| 6.3.2.5  | Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00                                    |   |                            |                              |
| 6.3.2.6  | ЭБС УМЦ ЖДТ по адресу https://umczdt.ru/books/  |   |                            |                              |
| 6.3.2.7  | ЭБС IPR SMART по адресу http://www.iprbookshop.ru/586.html  |   |                            |                              |
| 6.3.2.8  | Электронная библиотека диссертаций Российской государственной библиотеки по адресу https://dvs.rsl.ru/                      |   |                            |                              |

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

| Назначение   | Оснащение   |
|--|---|
| Учебная аудитория для проведения занятий лекционного типа, 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. Кабинет «Информатика, технологии и методы программирования». | 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<br>Технические средства обучения - Комплект мультимедийного оборудования |
| Учебная аудитория для проведения текущего контроля и промежуточной   | Специализированная мебель   |

|  |  |
|--|--|
| аттестации   |  |
| Учебная аудитория для проведения занятий лекционного типа  | Специализированная мебель<br>Демонстрационное оборудование - Комплект мультимедийного оборудования<br>Учебно-наглядные пособия - презентационные материалы   |
| Учебная аудитория для проведения групповых и индивидуальных консультаций   | Специализированная мебель  |
| Центр тестирования - Учебная аудитория для проведения текущего контроля и промежуточной аттестации   | Специализированная мебель<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   |
| 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   |
| 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<br>Лабораторное оборудование:<br>Аппаратно-программный комплекс шифрования "Континент"<br>Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе криптографические средства"<br>Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппаратные средства аутентификации пользователя<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<br>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, предусмотренной 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