ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.16 Программно-аппаратные средства защиты информации

рабочая программа дисциплины (модуля)

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

Учебный план 10.03.01 ИБ-2021.plx
10.03.01 Информационная безопасность

Направленность (профиль) Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 54
самостоятельная работа 90
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 7

Часов контактной работы всего, в том числе: 60,1
аудиторная работа 54
текущие консультации по лабораторным занятиям 1,8
текущие консультации по практическим занятиям 1,8
консультации перед экзаменом 2
прием экзамена 0,5

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Лабораторные	18	18	18	18
Практические	18	18	18	18
Элект	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	90	90	90	90
Сам. работа	90	90	90	90
Часы на контроль	36	36	36	36
Итого	216	216	216	216

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Цель дисциплины: Подготовить обучающегося к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники для организации защиты информации.
1.2	Задачи дисциплины: Получить представление о существующих программно-аппаратных средствах защиты информационных систем; умет устанавливать, кофигурировать и обслуживать программно-аппаратные средства информационных систем; получить представление о функционировании программных и аппаратных средств защиты информации в информационных системах.

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 дисциплин Теория информации, Безопасность сетей ЭВМ, Информационные технологии, Языки, технологии и методы программирования, Безопасность информационных процессов.
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 (эксплуатационная практика)
Производственная практика (преддипломная практика)
Комплексные системы защиты информации на транспорте
Управление информационной безопасностью на объектах транспортной инфраструктуры
Подготовка к процедуре защиты и защита выпускной квалификационной работы
Подготовка к сдаче и сдача государственного экзамена

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ОПК-2: Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности;
ОПК-2.1: Знает аппаратные средства вычислительной техники, принципы построения информационных систем и сетей, принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
ОПК-2.2: Знает и применяет информационно-коммуникационные технологии, принципы организации информационных систем и сетей в соответствии с требованиями по защите информации для решения задач профессиональной деятельности
ОПК-2.3: Осуществляет меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты информации
ОПК-2.4: Формирует и настраивает политику безопасности распространенных операционных систем, а также локальных вычислительных систем, построенных на их основе
ОПК-5: Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;

ОПК-5.2: Применяет нормативные правовые акты и нормативные методические документы по информационной безопасности в профессиональной деятельности
ОПК(п)-2.2: Способен формировать предложения по оптимизации структуры и функциональных процессов объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы;
ОПК(п)-2.2.1: Знает методы деструктивных воздействия на информационные ресурсы
ОПК(п)-2.2.2: Знает методы оценки устойчивости объектов защиты к деструктивным воздействиям на информационные ресурсы
ОПК(п)-2.2.3: Формирует предложения по оптимизации структуры и функциональных процессов объекта защиты
ОПК(п)-2.3: Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности;
ОПК(п)-2.3.3: Разрабатывает, внедряет и сопровождает комплекс мер по обеспечению безопасности объектов защиты различных видов
ОПК(п)-2.4: Способен проводить аудит защищенности объекта информатизации в соответствии с нормативными документами;
ОПК(п)-2.4.2: Знает и применяет нормативные документы в области аудита защищенности объекта информатизации
ОПК(п)-2.4.1: Применяет методики аудита защищенности объекта информатизации

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	Роль человеческого фактора в обеспечении защиты информации в автоматизированных системах /Лек/	7	2	ОПК(п)-2.2.1	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	
1.2	Особенности современных автоматизированных систем /Лек/	7	2	ОПК(п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	
1.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	18	ОПК(п)-2.2.1 ОПК (п)-2.2.3 ОПК-5.2 ОПК-2.1 ОПК-2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	

1.4	Уязвимости компьютерных систем /Пр/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.4.1 ОПК-2.1 ОПК-2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в гуппе. Освоение технологии
1.5	Знакомство со средами виртуализации систем /Лаб/	7	1	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в малых группах. Моделирование ситуаций
1.6	Подготовка отчета по лабораторной работе /Ср/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Управление доступом в компьютерных системах					
2.1	Криптографические требования к средствам защиты информации от несанкционированного доступа /Лек/	7	2	ОПК(п)-2.4.2 ОПК-2.1 ОПК-2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	
2.2	Управление доступом в операционных системах. Идентификация и аутентификация пользователей операционных систем /Пр/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	Работа в гуппе. Освоение технологии

2.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	16	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э4 Э5	
2.4	Конфигурирование системы защиты информации Dallas Lock /Лаб/	7	5	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в малых группах. изучение специализированного программного обеспечения
2.5	Применение системы защиты информации Secret Net Studio для организации защищенных компьютерных систем /Лаб/	7	5	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в малых группах. Изучение специализированного программного обеспечения
2.6	Конфигурирование защищенной сети ViPNet /Лаб/	7	7	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в малых группах. Изучение специализированного программного обеспечения

2.7	Подготовка отчетов по лабораторным работам /Ср/	7	8	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Защита информации от разрушающего воздействия вредоносных программ					
3.1	Состав и содержание документации политики безопасности /Лек/	7	2	ОПК-5.2 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	
3.2	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	10	ОПК-5.2 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
3.3	Антивирусные средства защиты и средства обнаружения вторжений /Пр/	7	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в группе. Освоение технологии
3.4	Подготовка к практическим занятиям /Ср/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. Обеспечение целостности информации					
4.1	Разграничение доступа к информации /Лек/	7	2	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э4 Э5	

4.2	Понятие компьютерного вируса. Специализированные средства и методы выявления вредоносных программ /Лек/	7	2	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-2.1 ОПК-2.2 ОПК-2.3	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э5	
4.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	2	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
4.4	Защита информации от несанкционированного доступа /Пр/	7	4	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в группе. Освоение технологии
4.5	Подготовка к практическим занятиям /Ср/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
	Раздел 5. Программно-аппаратные средства шифрования					
5.1	Средства обеспечения целостности информации. Электронная подпись /Лек/	7	2	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э5	
5.2	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	8	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	

5.3	Реализация программно-аппаратных средств, в соответствии с требованиями политики безопасности организации /Пр/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в группе. Освоение технологии
	Раздел 6. Защита современных информационных систем и сетей					
6.1	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	6	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э3 Э4 Э5	
6.2	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ /Лек/	7	2	ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3 Э4 Э5	
6.3	Защита корпоративной сетевой инфраструктуры /Пр/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э2 Э3 Э4 Э5	Работа в группе. Освоение технологии
6.4	Подготовка к практическим занятиям /Ср/	7	8	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	

	Раздел 7. Защита информации в электронных платежных системах					
7.1	Принципы организации электронных платежных систем /Лек/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
7.2	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	8	ОПК(п)-2.2.1 ОПК(п)-2.2.2	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э3 Э4 Э5	
7.3	Защита информации в системах электронной коммерции /Пр/	7	2	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э1 Э2 Э4 Э5	Работа вгруппе. Освоение технологии
7.4	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	7	36	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 Л3.2 Л3.3 Э5	
7.5	Промежуточная аттестация /Экзамен/	7	36	ОПК(п)-2.2.1 ОПК(п)-2.2.2 ОПК(п)-2.2.3 ОПК(п)-2.3.3 ОПК(п)-2.4.1 ОПК(п)-2.4.2 ОПК-5.2 ОПК-2.1 ОПК-2.2 ОПК-2.3 ОПК-2.4	Л1.1Л2.1Л3.1 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	Гузенкова Е. А.	Программно-аппаратные средства защиты информации: конспект лекций для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
6.1.2. Дополнительная учебная литература				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Шаньгин В.Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2020	http://znanium.com
6.1.3. Методические разработки				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А.	Программно-аппаратные средства защиты информации: методические указания к практическим занятиям для студентов направления подготовки бакалавриата 10.03.01 - «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.2	Гузенкова Е. А.	Программно-аппаратные средства защиты информации: методические рекомендации к самостоятельной работе для студентов направления подготовки бакалавриата 10.03.01 - «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru
Л3.3	Гузенкова Е. А.	Программно-аппаратные средства защиты информации: методические указания к лабораторным работам для студентов направления подготовки бакалавриата 10.03.01 «Информационная безопасность» очной формы обучения	Екатеринбург: УрГУПС, 2016	http://biblioserver.usurt.ru

6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)	
Э1	Сайт издательства КНОРУС (http://www.knorus.ru)
Э2	Информационно-консалтинговый центр по электронному бизнесу (http://www.e-commerce.ru)
Э3	Сайт по электронной коммерции и web-маркетингу Вадима Ельнина (http://www.vadimeidlin.com)
Э4	Система электронной поддержки обучения Blackboard Learn (http://bb.usurt.ru)
Э5	Официальный сат ФСТЭК России (http://www.fstec.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	ESET NOD32 Antivirus
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Система электронной поддержки обучения Blackboard Learn
6.3.1.8	Secret Net Studio
6.3.1.9	Система защиты информации от несанкционированного доступа: Dallas Lock
6.3.1.10	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 Компьютерная техника с установленным лицензионным ПО, предусмотренным пунктом 6.3.1 РПД, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель
Учебная аудитория для проведения занятий лекционного типа	Специализированная мебель Демонстрационное оборудование - Комплект мультимедийного оборудования Учебно-наглядные пособия - презентационные материалы
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
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 курсового проектирования (выполнения курсовых работ), самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций	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

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. Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя:- изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий);- подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".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).
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.