ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.15 Программно-аппаратные средства защиты информации

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) **6 ЗЕТ**

Часов по учебному плану 216
в том числе:
аудиторные занятия 72
самостоятельная работа 108
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 7

Часов контактной работы всего, в том числе: 79,9
аудиторная работа 72
текущие консультации по лабораторным занятиям 3,6
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	РПД	УП	РПД
Лекции	18	18	18	18
Лабораторные	36	36	36	36
Практические	18	18	18	18
Контактная работа	72	72	72	72
Итого ауд.	72	72	72	72
Сам. работа	108	108	108	108
Часы на контроль	36	36	36	36
Итого	216	216	216	216

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Подготовить обучающегося к деятельности, связанной с эксплуатацией и обслуживанием аппаратуры и оборудования, содержащего современные средства вычислительной техники для организации защиты информации.

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, Криптографические методы защиты информации.
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)
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 угроз информационной безопасности и возможные пути их реализации
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации
Уровень 2	-
Уровень 3	-
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-1: способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации

Знать:	
Уровень 1	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
Уровень 2	принципы организации информационных систем в соответствии с требованиями по защите информации

Уровень 3	принцыпы формирования политики информационной безопасности в информационных системах
Уметь:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Владеть:	
Уровень 1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов
Уровень 2	методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем
Уровень 3	навыками участия в экспертизе состояния защищенности информации на объекте защиты

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Знать:	
Уровень 1	аппаратные средства вычислительной техники; принципы построения информационных систем; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации
Уровень 2	назначение, функции и структуру операционных систем
Уровень 3	принцыпы организации информационных систем в соотвествии с требованиями по защите информации
Уметь:	
Уровень 1	выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах
Уровень 2	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Уровень 3	формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных систем, построенных на их основе
Владеть:	
Уровень 1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов
Уровень 2	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
Уровень 3	навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Уровень 2	оценить конфигурацию системы и дать рекомендации по усилению мер защиты
Уровень 3	осуществить меры по изменению системы на основе полученных выводов
Владеть:	
Уровень 1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов
Уровень 2	метдами мониторинга и аудита, выявления угроз информационной безопасности информационных систем
Уровень 3	методами управления информационной безопасностью информационных систем

ПСК-2: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты

Уровень 2	оценивать уровень угрозы системе и дать обоснование необходитмости усиления мер защиты системы
Уровень 3	составить на основе выявленных нарушений план по предотвращению новых аттак на основе арализа существующей ситуации
Владеть:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

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	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э4	
1.2	Особенности современных автоматизированных систем /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Э1 Э4	
1.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	18	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э4	
1.4	Уязвимость компьютерных систем /Пр/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	
1.5	Знакомство со средами виртуализации систем /Лаб/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2 ОПК-7	Л1.2Л2.2Л3.3 Э1 Э2 Э3 Э4	Работа в малых группах. Анализ практико-ориентированных задач. Моделирование ситуаций
1.6	Подготовка отчета по лабораторной работе /Ср/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2 ОПК-7	Л1.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Э1 Э2 Э3 Э4	

	Раздел 2. Управление доступом в компьютерных системах					
2.1	Криптографические требования к средствам защиты информации от несанкционированного доступа /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.2 Э1 Э4	
2.2	Управление доступом в операционных системах. Идентификация и аутентификация пользователей операционных систем /Пр/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.1 Э1 Э4	
2.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	16	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э4	
2.4	Конфигурирование системы защиты информации Dallas Lock /Лаб/	7	10	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.3 Э1 Э2 Э3 Э4	Работа в малых группах. Анализ практико-ориентированных задач. Моделирование ситуаций
2.5	Применение системы защиты информации Secret Net Studio для организации защищенных компьютерных систем /Лаб/	7	10	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.3 Э1 Э2 Э3 Э4	Работа в малых группах. Анализ практико-ориентированных задач. Моделирование ситуаций
2.6	Конфигурирование защищенной сети ViPNet /Лаб/	7	14	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.3 Э1 Э2 Э3 Э4	
2.7	Подготовка отчетов по лабораторным работам /Ср/	7	8	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 3. Защита информации от разрушающего воздействия вредоносных программ					
3.1	Состав и содержание документации политики безопасности /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Э1 Э4	
3.2	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	14	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
3.3	Антивирусные средства защиты и средства обнаружения вторжений /Пр/	7	4	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	
3.4	Подготовка к практическим занятиям /Ср/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2 ОПК-7	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Э1 Э2 Э3 Э4	
	Раздел 4. Обеспечение целостности информации					

4.1	Разграничение доступа к информации /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Э1 Э4	
4.2	Понятие компьютерного вируса. Специализированные средства и методы выявления вредоносных программ /Лек/	7	2	ПК-2 ОПК-7	Л1.2Л2.2	
4.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
4.4	Защита информации от несанкционированного доступа /Пр/	7	4	ПК-1 ПК-2 ПК-3 ПСК-2 ОПК-7	Л1.2Л2.2Л3.1 Э1 Э2 Э3 Э4 Э5	Анализ практико-ориентированных задач. Моделирование ситуаций. Групповая дискуссия.
4.5	Подготовка к практическим занятиям /Ср/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2 ОПК-7	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Э1 Э2 Э3 Э4	
	Раздел 5. Программно-аппаратные средства шифрования					
5.1	Способы и средства обеспечения целостности информации /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1 Э1 Э4	
5.2	Средства защиты целостности информации. Электронная подпись /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2	
5.3	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	18	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
5.4	Реализация программно-аппаратных средств, в соответствии с требованиями политики безопасности организации /Пр/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1Л3.1 Э1 Э2 Э3 Э4 Э5	Анализ практико-ориентированных задач. Моделирование ситуаций. Групповая дискуссия.
	Раздел 6. Защита современных информационных систем и сетей					
6.1	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	6	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э3 Э4	
6.2	Программно-аппаратные методы и средства ограничения к ресурсам и компонентам ПЭВМ /Лек/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Э2 Э3 Э4	

6.3	Защита корпоративной сетевой инфраструктуры /Пр/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.1 Э2 Э3 Э4 Э5	Анализ практико-ориентированных задач. Моделирование ситуаций. Групповая дискуссия.
6.4	Подготовка к практическим занятиям /Ср/	7	12	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
	Раздел 7. Защита информации в электронных платежных системах					
7.1	Изучение литературы и нормативных документов по тематике раздела /Ср/	7	8	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л3.2 Э1 Э2 Э3 Э4	
7.2	Защита информации в системах электронной коммерции /Пр/	7	2	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.2Л2.2Л3.1 Э1 Э2 Э4	Анализ практико-ориентированных задач. Моделирование ситуаций. Групповая дискуссия.
7.3	Промежуточная аттестация /Экзамен/	7	36	ПК-1 ПК-2 ПК-3 ПСК-2	Л1.1 Л1.2Л2.1 Л2.2Л3.1 Л3.2 Л3.3 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	Крамаров С.О., Тищенко Е.Н.	Криптографическая защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2018	http://znanium.com/catalog/product/901659
Л1.2	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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка

Л2.1	Бабаш А. В.	Криптографические методы защиты информации. Том 3: Учебно-методическое пособие	Москва: Издательский Центр РИО, 2014	http://znanium.com/catalog/product/432654
Л2.2	Шаньгин В. Ф.	Информационная безопасность компьютерных систем и сетей: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2017	http://znanium.com/catalog/product/775200
Л2.3		Методические документы. Профили защиты средств антивирусной защиты.	Утв. ФСТЭК России 14.06.2012 г.	http://www.consultant.ru/document/cons_doc_LAW_180640/
Л2.4		Методические документы. Профили защиты систем обнаружения вторжений	Утв. ФСТЭК России 06.03.2012 г.	http://www.consultant.ru/document/cons_doc_LAW_180345/
Л2.5		Методические документы. Профили защиты систем обнаружения вторжений	Утв. ФСТЭК России 03.02.2012 г.	http://www.consultant.ru/document/cons_doc_LAW_180342/
Л2.6		Методические документы. Профили защиты средств доверенной загрузки	Утв. ФСТЭК России 30.12.2013 г.	http://www.consultant.ru/document/cons_doc_LAW_159034/
Л2.7		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.8		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.9		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.10		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist
Л2.11		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist
Л2.12		Каталог учебных, учебно-методических пособий, научных и других изданий вузов железнодорожного транспорта: справочно-библиографическое издание	Москва, ФГБУ ДПО «УМЦ ЖДТ» 2018	http://www.usurt.ru/izdatelsko-bibliotechnyy-kompleks/bibliotechno-informacionnuy-center/katalog-fgbou-umts-zhdt
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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
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/cgi-bin/irbis64r_13/cgiirbis_64.exe?C21COM=F&I21DBN=KN&P21DBN=KN
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/cgi-bin/irbis64r_13/cgiirbis_64.exe?LNG=&P21DBN=KN&I21DBN=KN

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". Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе криптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппаратные средства аутентификации 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.
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).