

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

Б1.В.ДВ.04.02 Защита информационных процессов на транспорте

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)	5 ЗЕТ		
Часов по учебному плану	180	Часов контактной работы всего, в том числе:	60,1
в том числе:		аудиторная работа	54
аудиторные занятия	54	текущие консультации по практическим занятиям	3,6
самостоятельная работа	90	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	
	Неделя			
Неделя	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	36	36	36	36
Итого ауд.	54	54	54	54
Контактная работа	54	54	54	54
Сам. работа	90	90	90	90
Часы на контроль	36	36	36	36
Итого	180	180	180	180

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Формирование знаний и умений по обеспечению информационной безопасности компьютерных систем и информационных процессов, и навыков по их определению для конкретных условий.
-----	---

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП

Цикл (раздел) ОП:	Б1.В.ДВ.04
-------------------	------------

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные при изучении дисциплин Теория информации, Организационное и правовое обеспечение информационной безопасности, Техническая защита информации, Безопасность информационных процессов, Безопасность сетей ЭВМ, Теория информационной безопасности и методология защиты информации, Стеганография, Криптографические методы защиты информации.

В результате освоения предшествующих дисциплин обучающийся должен знать: принципы построения криптографических алгоритмов, криптографические стандарты и их использование в информационных системах; принципы построения информационных систем; принципы организации информационных систем в соответствии с требованиями по защите информации; назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ, основные понятия и методы математической логики и теории алгоритмов диспетчеризации, способы проверки операционных систем на безопасность использования различных программных и аппаратных средств; основы администрирования вычислительных сетей; системы управления базами данных;

уметь: использовать программные и аппаратные средства персонального компьютера; 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; 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;

владеть: навыками применения современных информационных технологий в профессиональной деятельности; методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации; методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений; навыками выявления и уничтожения компьютерных вирусов.

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**ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты****Знать:**

Уровень 1	состав подсистем информационной безопасности объекта защиты
Уровень 2	методы администрирования подсистем информационной безопасности объекта защиты
Уровень 3	способы администрирования подсистем информационной безопасности объекта защиты

Уметь:

Уровень 1	определять подсистемы комплексной системы защиты информации
Уровень 2	администрировать подсистемы комплексной системы защиты информации
Уровень 3	-

Владеть:

Уровень 1	методами и способами администрирования подсистем информационной безопасности 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	понятие политики безопасности
Уровень 2	порядок разработки политики безопасности
Уровень 3	порядок реализации политики безопасности

Уметь:

Уровень 1	разрабатывать политику безопасности
Уровень 2	реализовывать политику безопасности
Уровень 3	оценивать эффективность выполнения политики безопасности

Владеть:	
Уровень 1	навыками выполнения работ по реализации политики безопасности
Уровень 2	-
Уровень 3	-

ПК-6: способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации

Знать:	
Уровень 1	основные угрозы безопасности информации и модели нарушителя в информационных системах.
Уровень 2	методы аттестации уровня защищенности информационных систем.
Уровень 3	принципы формирования политик безопасности в информационных системах.
Уметь:	
Уровень 1	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.
Уровень 2	разрабатывать модели угроз и нарушителей информационной безопасности информационных систем.
Уровень 3	контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем.
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 эффективности функционирования защищенных информационных систем.
Уровень 3	навыками участия в экспертизе состояния защищенных информационных систем.

ПК-10: способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности

Знать:	
Уровень 1	основные принципы построения комплексных систем информационной безопасности.
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 частные 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.

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Знать:	
Уровень 1	основные методы управления информационной безопасностью.
Уровень 2	основные угрозы безопасности информации и модели информационных систем.
Уровень 3	принципы формирования политики информационной безопасности в информационных системах.
Уметь:	
Уровень 1	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.
Уровень 2	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.
Уровень 3	контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем.
Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры информационных систем 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.

ПК-15: способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Знать:

Уровень 1	нормативные документы ФСБ России, ФСТЭК России
Уровень 2	-
Уровень 3	-

Уметь:

Уровень 1	организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными документами ФСБ России, ФСТЭК России
Уровень 2	-
Уровень 3	-

Владеть:

Уровень 1	-
Уровень 2	-
Уровень 3	-

ПК-1: способностью формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности, административно-управленческой и технической реализуемости и экономической целесообразности

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.

ПК-4: способностью собрать и провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности

Знать:

Уровень 1	основные стандарты проектирования информационных систем.
Уровень 2	основы проектирования систем защиты информации.
Уровень 3	состав исходных данных для проектирования информационных систем.

Уметь:

Уровень 1	собрать исходные данные для проектирования подсистем и средств обеспечения информационной безопасности.
Уровень 2	провести анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.
Уровень 3	провести технико-экономическое обоснование проектного решения.

Владеть:

Уровень 1	навыками сбора исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.
Уровень 2	навыками проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности.
Уровень 3	навыками проведения технико-экономического обоснования проектного решения.

ПК-6: способностью формировать комплекс мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью

Знать:

Уровень 1	основные принципы построения комплексных систем защиты информации.
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.
3.2	Уметь:
3.2.1	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты;
3.2.2	анализировать и оценивать угрозы информационной безопасности;
3.2.3	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
3.3	Владеть:
3.3.1	методами и средствами выявления угроз безопасности автоматизированным системам;
3.3.2	методами формирования требований по защите информации;
3.3.3	методами анализа и формализации информационных процессов объекта и связей между ними;
3.3.4	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. Общие положения об информационной безопасности для телекоммуникационных систем					
1.1	Виды угроз информационной безопасности в телекоммуникационных системах /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.2	VPN как средство информационной безопасности /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.3	Варианты построения и средства защиты информации, дополняющие VPN /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	

1.4	Состав программно-аппаратного комплекса ViPNet /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.5	Логическая структура сети ViPNet. Понятия адресной и прикладной администрации. Особенности ключевой структуры сети ViPNet /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.6	Практический семинар /Пр/	7	6	ПК-10 ПСК-1 ПСК-6	Л1.1Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	Групповая дискуссия
1.7	Подготовка к практическому семинару /Ср/	7	8	ПК-10 ПСК-1 ПСК-6	Л1.1Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
1.8	Изучение литературы по тематике раздела /Ср/	7	10	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 Э5	
Раздел 2. ViPNet [Администратор] и его основные модули						
2.1	Ключевой и удостоверяющий центр ViPNet (УКЦ) /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
2.2	Особенности взаимодействия ЦУС и УКЦ /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
2.3	Состав файла-дистрибутива /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
2.4	Практический семинар /Пр/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	Групповая дискуссия
2.5	Подготовка к практическому семинару /Ср/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	

2.6	Изучение литературы по тематике раздела /Ср/	7	10	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
Раздел 3. ViPNet [Координатор] и его основные модули						
3.1	Функции ViPNet [Координатора]. Настройки координатора /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
3.2	Логика использования виртуальных адресов /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
3.3	Практический семинар /Пр/	7	6	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	Групповая дискуссия
3.4	Подготовка к практическому семинару /Ср/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
3.5	Изучение литературы по тематике раздела /Ср/	7	10	ПК-10 ПСК-1 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 Э5	
Раздел 4. ViPNet [Клиент] - характеристика и основные функции						
4.1	Персональный сетевой экран /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
4.2	Установление защищенных соединений /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
4.3	Услуги защищенных служб реального времени /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	

4.4	Сервис защищенных почтовых услуг /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
4.5	Практический семинар /Пр/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	Групповая дискуссия
4.6	Подготовка к практическому семинару /Ср/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4	
4.7	Изучение литературы по тематике раздела /Ср/	7	10	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 Э5	
Раздел 5. Типовые схемы применения технологии ViPNet						
5.1	Практический семинар /Пр/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.1 Л2.2 Л2.3Л3.1 Э1 Э2 Э3 Э4 Э5	Групповая дискуссия
5.2	Подготовка к практическому семинару /Ср/	7	8	ПК-10 ПСК-1 ПСК-6	Л2.1 Л2.2 Л2.3Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5	
5.3	Изучение литературы по тематике раздела /Ср/	7	10	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 Э5	
5.4	Промежуточная аттестация /Экзамен/	7	36	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1Л2.2 Л2.3Л3.2 Э1 Э2	

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
---------------------	----------	-------------------	------------

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Зырянова Т. Ю.	Защита информационных процессов на транспорте: конспект лекций для студентов направления подготовки 10.03.01 «Информационная безопасность»	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		Кодексы и Законы Российской Федерации: официальное издание	СПб.: Весь, 2007	
Л2.2	Максимов Н. В., Попов И. И.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2018	http://znanium.com
Л2.3	Кузин А. В., Кузин Д.А.	Компьютерные сети: Учебное пособие	Москва: Издательство "ФОРУМ", 2018	http://znanium.com

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Зырянова Т. Ю.	Защита информационных процессов на транспорте: методические рекомендации к практическим семинарам по дисциплине «Защита информационных процессов на транспорте» 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.	Защита информационных процессов на транспорте: методические рекомендации по организации самостоятельной работы по дисциплине «Защита информационных процессов на транспорте» 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	Официальный сайт ОАО "ИнфоТекС" (http://www.infotecs.ru)
Э2	Система электронной поддержки обучения Blackboard Learn (http://bb.usurt.ru)
Э3	Официальный сайт ФСТЭК России (http://www.fstec.ru)
Э4	Официальный сайт ФСБ России (http://www.fsb.ru)
Э5	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	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	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
6.3.2.5	Международная реферативная база данных научных изданий Scopus
6.3.2.6	Международная реферативная база данных научных изданий eLIBRARY.RU
6.3.2.7	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.8	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
Компьютерный класс - Учебная аудитория для самостоятельной работы студентов	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
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Технические средства обучения - Комплект мультимедийного оборудования
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

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ) И ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)
<p>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.</p> <p>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»).</p> <p>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.</p> <p>Пользование информационными ресурсами расширяет возможности освоения теоретического курса, выполнения самостоятельной работы и позволяет получить информацию для реализации творческих образовательных технологий.</p> <p>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), доступной через личный кабинет обучающегося.</p> <p>Методические материалы, разработанные для обеспечения образовательного процесса представлены в электронном каталоге УрГУПС.</p> <p>Формы самостоятельной работы студентов по данной дисциплине разнообразны. Они включают в себя:</p> <ul style="list-style-type: none"> - 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).