ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.В.ДВ.04.01 Комплексные системы защиты информации 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
в том числе:
аудиторные занятия 54
самостоятельная работа 90
часов на контроль 36

Часов контактной работы всего, в том числе: 60,1
аудиторная работа 54
текущие консультации по практическим занятиям 3,6
консультации перед экзаменом 2
прием экзамена 0,5

Промежуточная аттестация и формы контроля:
экзамен 7

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Лекции	18	18	18	18
Практические	36	36	36	36
Контактная работа	54	54	54	54
Итого ауд.	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	Изучение методологических и законодательных основ организации комплексной системы защиты информации на предприятии, основных аспектов деятельности по ее созданию, обеспечению функционирования и контролю эффективности. Изучение структуры комплексной системы защиты информации на предприятии. Обобщение основополагающих нормативно-правовых принципов организации системы защиты информации.
1.2	Изучение методов проведения анализа и управления информационными рисками предприятия.

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 информационных систем; основные нормативные правовые акты в области информационной безопасности и защиты информации; нормативные методические документы Федеральной службы по техническому и экспортному контролю; правовые соновы защиты конфиденциальной информации; принципы и методы организационной защиты информации; технические каналы утечки информации, возможности технических разведок, способы и средства защиты информации от утечки по техническим каналам, методы и средства контроля эффективности технической защиты информации; принципы организации информационных систем в соответствии с требованиями по защите информации;
уметь: пользоваться нормативными документами по защите информации;
владеть: навыками работы с нормативными правовыми актами; методами технической защиты информации; методами расчета и инструментального контроля показателей технической защиты 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	
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	способыадминистрирования 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 полдитики 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 эффектиности 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
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	-

ПСК-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 обснования критериев эффективности функционирования защищенных информационных систем
Уровень 2	навыками организации информационных систем в соответствии с требованиями по защите информации
Уровень 3	-

ПСК-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

ПСК-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 проетирования, 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 докмуентов.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература	Активные формы
	Раздел 1. Методология КСЗИ на предприятии					
1.1	Системный подход к обеспечению информационной безопасности /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
1.2	Государственная система защиты информации в Российской Федерации /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2 Э3 Э4 Э5	
1.3	Сущность и задачи КСЗИ на предприятии /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
1.4	Принципы организации КСЗИ на предприятии /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
1.5	Общая модель КСЗИ /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	

1.6	Формирование требований к КСЗИ /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
1.7	Обеспечение транспортной безопасности в части применения технических средств защиты. Видеохранные системы /Пр/	7	18	ПК-6 ПК-13 ПСК-6 ПК-3 ПК-15	Л1.1Л2.1 Л2.2 Л2.3Л3.2 Э1 Э2 Э3 Э4 Э5	Работа в группе, решение практико-ориентированных задач
1.8	Обеспечение транспортной безопасности в части применения технических средств защиты. Пожарно-охранная сигнализация /Пр/	7	18	ПК-6 ПК-13 ПСК-6 ПК-3 ПК-15	Л1.1Л2.1 Л2.2 Л2.3Л3.3 Э1 Э2 Э3 Э4 Э5	Работа в группе, решение практико-ориентированных задач
1.9	Изучение литературы и документов по тематике раздела /Ср/	7	32	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	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 Л2.13 Л2.14 Л3.1 Э1 Э2 Э3 Э4 Э5	
	Раздел 2. Управление КСЗИ					
2.1	Управление процессами функционирования КСЗИ. Общая модель управления. Планирование защиты /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
2.2	Управление процессами функционирования КСЗИ. Оперативное управление. Календарно-плановое руководство /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
2.3	Разработка политики безопаности /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
2.4	Изучение литературы и документов по тематике раздела /Ср/	7	20	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2 Э3 Э4 Э5	
	Раздел 3. Основы управления информационными рисками					
3.1	Основные понятия и принципы управления информационными рисками /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	

3.2	Классификация видов ущерба и риска /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
3.3	Классификация методов управления информационными рисками /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
3.4	Методика матрицы рисков /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
3.5	Экспертные методики анализа информационных рисков /Лек/	7	1	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
3.6	Изучение литературы и документов по тематике раздела /Ср/	7	20	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2 Э3 Э4 Э5	
	Раздел 4. Эффективность КСЗИ					
4.1	Системный подход к оценке эффективности КСЗИ /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
4.2	Экономический подход к оценке эффективности КСЗИ /Лек/	7	2	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Э1 Э2 Э3 Э4 Э5	
4.3	Изучение литературы и документов по тематике раздела /Ср/	7	18	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-4	Л1.1 Л1.2Л2.2 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л3.1 Э1 Э2 Э3 Э4 Э5	
4.4	Промежуточная аттестация /Экзамен/	7	36	ПК-6 ПК-10 ПК-13 ПСК-1 ПСК-4 ПСК-6 ПК-3 ПК-4 ПК-15	Л1.1 Л1.2Л2.1 Л2.2 Л2.3Л3.1 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	Шаньгин В. Ф.	Комплексная защита информации в корпоративных системах: Учебное пособие	Москва: Издательский Дом "ФОРУМ", 2018	http://znanium.com/catalog/product/937502
Л1.2	Зырянова Т. Ю.	Комплексные системы защиты информации на транспорте: конспект лекций 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

6.1.2. Дополнительная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1		Кодексы и Законы Российской Федерации: официальное издание	СПб.: Весь, 2007	
Л2.2	Гришина Н.В.	Комплексная система защиты информации на предприятии: Учебное пособие	Москва: Издательство "ФОРУМ", 2009	http://znanium.com/catalog/product/175658
Л2.3		Федеральный закон: Выпуск 2 (510). О безопасности	Москва: Издательский Дом "ИНФРА-М",	http://znanium.com/catalog/product/221935
Л2.4		Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 "Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" (с изменениями и дополнениями)	утв. ФСТЭК России 14.03.2014 г.	http://www.consultant.ru/document/cons_doc_LAW_165503/
Л2.5		Федеральный закон от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"		http://www.consultant.ru/document/cons_doc_LAW_220885/
Л2.6		Федеральный закон от 9 февраля 2007 г. N 16-ФЗ "О транспортной безопасности" (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_66069/
Л2.7		Методический документ "Меры защиты информации в государственных информационных системах"	утв. ФСТЭК России 11.02.2014 г.	http://www.consultant.ru/document/cons_doc_LAW_159975/

Л2.8		Приказ ФСБ РФ от 9 февраля 2005 г. N 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»	утв. ФСБ России 09.02.2005 г.	http://www.consultant.ru/document/cons_doc_LAW_52098/
Л2.9		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.10		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.11		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.12		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist
Л2.13		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist
Л2.14		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	Зырянова Т. Ю.	Комплексные системы защиты информации на транспорте: методические рекомендации по организации самостоятельной работы по дисциплине «Комплексные системы защиты информации 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	Черенев Ю. Б.	Видеоохранные системы: практикум по дисциплине «Комплексные системы защиты информации на транспорте» 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
Л3.3	Черенев Ю. Б.	Пожарно-охранная сигнализация: методические рекомендации к практическим занятиям по дисциплине «Комплексные системы защиты информации на транспорте» 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

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

Э1	Информационный портал по стандартам в области информационной безопасности (http://www.iso27000.ru)
Э2	Официальный сайт ФСТЭК России (http://www.fstec.ru)
Э3	Среда электронного обучения BlackBoard Learn
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	Программное обеспечение компьютерного тестирования АСТ
6.3.1.4	Система электронной поддержки обучения Blackboard Learn
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Справочно-правовая система КонсультантПлюс
6.3.2.2	Справочно-правовая система Гарант
6.3.2.3	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.4	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
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
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)

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).