ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.Б.18 Техническая защита 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) **8 ЗЕТ**

Часов по учебному плану 288
в том числе:
аудиторные занятия 90
самостоятельная работа 162
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 6 зачет с оценкой 5 КП 5

Часов контактной работы всего, в том числе: 101,15
аудиторная работа 90
текущие консультации по лабораторным занятиям 3,6
текущие консультации по практическим занятиям 2,8
консультации перед экзаменом 2
прием экзамена 0,5
прием зачета с оценкой 0,25
проверка, защита курсового проекта 2

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**5 (3.1)**		**6 (3.2)**		Итого	
Недель	18		18			
Вид занятий	УП	РПД	УП	РПД	УП	РПД
Лекции	18	18	8	8	26	26
Лабораторные	18	18	18	18	36	36
Практические	18	18	10	10	28	28
Контактная работа	54	54	36	36	90	90
Итого ауд.	54	54	36	36	90	90
Сам. работа	90	90	72	72	162	162
в том числе КП	36	36			36	36
Часы на контроль			36	36	36	36
Итого	144	144	144	144	288	288

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1	Ознакомить обучающихся с основными аспектами технической защиты информации, начиная от свойств информации как предмета защиты, ее источников и носителей до методологии защиты информации применительно к конкретным условиям. Способствовать формированию у обучающихся комплексного понимания вопроса 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 волновых процессов, Физические основы защиты информации, Электротехника, электроника и схемотехника, Теория информационной безопасности и методология защиты информации.
В результате освоения предшествующих дисциплин обучающийся должен знать: основные понятия, законы и модели теории колебаний и волн; основные физические законы в области электричества и магнетизма;
уметь: применять основные законы физики при решении прикладных задач; рассчитывать параметры полупроводниковых и электронных приборов;
владеть: навыками проведения физического эксперимента и обработки его результатов.

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Комплексные системы защиты информации на транспорте
Защита информационных процессов на транспорте
Производственная практика (проектно-технологическая практика)
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 защищаемой информации
Уровень 2	классификацию угроз защищаемой информации
Уровень 3	возможные методы и пути реализации угроз защищаемой информации
Уметь:	
Уровень 1	выявлять угрозы информационной безопасности объекта
Уровень 2	анализировать угрозы информационной безопасности объекта
Уровень 3	оценивать угрозы информационной безопасности объекта
Владеть:	
Уровень 1	методами и средствами выявления угроз информационной безопасности объекта
Уровень 2	методами и средствами анализа информационной безопасности объекта
Уровень 3	методами и средствами оценки информационной безопасности объекта

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	аппаратные средства вычислительной техники
Уровень 2	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы организации информационных систем в соответствии с требованиями по защите информации
Уровень 3	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
Уметь:	
Уровень 1	-
Уровень 2	-
Уровень 3	анализировать и оценивать угрозы информационной безопасности объекта
Владеть:	
Уровень 1	профессиональной терминологией, навыками чтения электронных схем, навыками безопасного использования технических средств в профессиональной деятельности
Уровень 2	навыками работы с нормативными правовыми актами; методами технической защиты информации

Уровень 3	методами расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знать:	
Уровень 1	основные принципы построения комплексных систем защиты информации
Уровень 2	основные угрозы безопасности информации и модели нарушителя в информационных системах предприятий в различных сферах
Уровень 3	принципы формирования и реализации политики безопасности в информационных системах предприятий различных сфер деятельности
Уметь:	
Уровень 1	определять информационную инфраструктуру и информационные ресурсы предприятия, подлежащие защите
Уровень 2	разрабатывать модели угроз и модели нарушителей информационной безопасности информационных систем предприятий в различных сферах деятельности
Уровень 3	определять комплекс мер для обеспечения информационной безопасности информационных систем предприятий различных сфер
Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры предприятий различных сфер деятельности
Уровень 2	методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем предприятий различных сфер деятельности
Уровень 3	навыками выбора комплекса мер для обеспечения информационной безопасности информационных систем предприятий различных сфер деятельности

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
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

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-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	
Знать:	
Уровень 1	аппаратные средства вычислительной техники
Уровень 2	принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации; принципы организации информационных систем в соответствии с требованиями по защите информации
Уровень 3	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
Уметь:	
Уровень 1	-
Уровень 2	-
Уровень 3	анализировать и оценивать угрозы информационной безопасности объекта
Владеть:	
Уровень 1	профессиональной терминологией, навыками чтения электронных схем, навыками безопасного использования технических средств в профессиональной деятельности
Уровень 2	навыками работы с нормативными правовыми актами; методами технической защиты информации
Уровень 3	методами расчета и инструментального контроля показателей технической защиты информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
Знать:	
Уровень 1	основные методы управления информационной безопасностью
Уровень 2	методы аттестации уровня защищенности информационных систем
Уровень 3	принципы формирования политики информационной безопасности в информационных системах
Уметь:	
Уровень 1	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Уровень 2	выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем
Уровень 3	определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем
Владеть:	
Уровень 1	навыками организации и обеспечения режима секретности
Уровень 2	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
Уровень 3	-

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Знать:	
Уровень 1	принципы формирования политики информационной безопасности в информационных системах
Уровень 2	основные угрозы безопасности информации и модели нарушителя в информационных системах
Уровень 3	основные методы управления информационной безопасностью, методы аттестации уровня защищенности информационных систем
Уметь:	
Уровень 1	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; разрабатывать модели угроз и нарушителей информационной безопасности информационных систем; оценивать информационные риски в информационных системах
Уровень 2	выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности информационных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности информационных систем

Уровень 3	разрабатывать частные политики информационной безопасности информационных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности информационных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью информационных систем
Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры информационной системы и ее безопасностию; методами мониторинга и аудита, выявления угроз информационной безопасности информационных систем
Уровень 2	основами методов управления информационной безопасностью информационных систем
Уровень 3	навыками выбора и обоснования критериев эффективности функционирования защищенных информационных систем

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	основы организационного и правового обеспечения информационной безопасности, основные нормативные правовые акты в области обеспечения информационной безопасности и нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
Уровень 2	правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны и служб защиты информации на предприятиях
Уровень 3	организацию работы и нормативные правовые акты и стандарты по лицензированию деятельности в области обеспечения защиты государственной тайны, технической защиты конфиденциальной информации, по аттестации объектов информатизации и сертификации средств защиты информации
Уметь:	
Уровень 1	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Уровень 2	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Уровень 3	определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите
Владеть:	
Уровень 1	навыками работы с нормативными правовыми актами
Уровень 2	навыками организации и обеспечения режима секретности
Уровень 3	методами формирования требований по защите информации

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	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;
3.1.2	методы и приборы для предотвращения возможности утечки информации.
3.2	**Уметь:**
3.2.1	выявлять и анализировать угрозы безопасности информации;
3.2.2	формулировать требования к способам и средствам защиты информации инженерно-техническими средствами применительно к конкретным условиям;
3.2.3	среди множества выбрать и предложить рациональные способы и средства защиты с требуемым уровнем защиты при минимальных затратах.
3.3	**Владеть:**
3.3.1	методами формирования требований по защите информации;
3.3.2	методами проведения специальных исследований технических средств, на которых ведется обработка, хранение и передача конфиденциальной информации;
3.3.3	методами проведения обследований помещений для вынесения заключений о защищенности объекта и выявления технических каналов утечки информации;
3.3.4	методами оценки эффективности применяемых средств и мер инженерно-технической защиты.

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)						
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов (академических)**	**Компетенции**	**Литература**	**Активные формы**
	Раздел 1. Свойства и виды защищаемой информации					

1.1	Понятие об информации как предмете защиты. Основные свойства информации как предмета защиты. Информация как товар. Изменение во времени ценности информации. Количество информации и качество. Копирование (тиражирование) информации. Виды защищаемой информации. /Лек/	5	4	ОПК-7	Л1.1Л2.1 Л2.2 Э1 Э2 Э3	
1.2	Технология защиты речевой информации в помещениях /Пр/	5	4	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
1.3	Анализ двухпроводных телефонных линий на наличие несанкционированных подключений /Лаб/	5	4	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
1.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	5	6	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.3 Э1 Э2 Э3	
	Раздел 2. Демаскирующие признаки объекта защиты					
2.1	Классификация демаскирующих признаков и их виды. Видовые демаскирующие признаки. Демаскирующие признаки сигналов. Демаскирующие признаки веществ. /Лек/	5	4	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	
2.2	Технология защиты речевой информации в помещениях /Пр/	5	4	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
2.3	Анализ двухпроводных телефонных линий на наличие несанкционированных подключений /Лаб/	5	4	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
2.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	5	6	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.3 Э1 Э2 Э3	
	Раздел 3. Источники и носители информации					

3.1	Виды источников информации. Источники функциональных сигналов. Побочные излучения и наводки. Классификация типов средств источников опасных сигналов. Акустоэлектрические преобразователи. Пьезоэлектрические преобразователи. Побочные электромагнитные излучения персонального компьютера и защита информации. Паразитные связи и наводки. /Лек/	5	4	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	
3.2	Технология защиты речевой информации в помещениях /Пр/	5	2	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
3.3	Анализ двухпроводных телефонных линий на наличие несанкционированных подключений /Лаб/	5	2	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
3.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	5	8	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.3 Э1 Э2 Э3	
	Раздел 4. Угрозы безопасности информации. Виды угроз безопасности информации					
4.1	Основные непреднамеренные искусственные угрозы. Основные преднамеренные искусственные угрозы. /Лек/	5	2	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	
4.2	Технология защиты речевой информации в помещениях /Пр/	5	4	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
4.3	Анализ двухпроводных телефонных линий на наличие несанкционированных подключений /Лаб/	5	4	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
4.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	5	8	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.3 Э1 Э2 Э3	
	Раздел 5. Органы добывания информации. Принципы, технология добывания информации					

5.1	Органы добывания информации. Принципы добывания информации. Технология добывания информации. Информационная или аналитическая работа. Способы несанкционированного доступа к конфиденциальной информации. Добывание информации без физического проникновения в контролируемую зону. показатели эффективности добывания информации. /Лек/	5	4	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	
5.2	Технология защиты речевой информации в помещениях /Пр/	5	4	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
5.3	Анализ двухпроводных телефонных линий на наличие несанкционированных подключений /Лаб/	5	4	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
5.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	5	8	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.3 Э1 Э2 Э3	
5.5	Выполнение и подготовка к защите курсового проекта /Ср/	5	36	ОПК-7 ПК-4 ПК-11 ПК-13	Л1.1Л2.1 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 Л2.15 Л3.3 Э1 Э2 Э3	
5.6	Подготовка к промежуточной аттестации /Ср/	5	18	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Л3.1 Л3.2 Л3.3 Э1 Э2 Э3	
	Раздел 6. Технические каналы утечки информации					
6.1	Особенности утечки информации. Характеристики технических каналов утечки информации. Классификация и краткая характеристика технических каналов утечки информации. Оптический канал утечки информации. Радиоэлектронный канал утечки информации. Акустический канал утечки информации. /Лек/	6	4	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	

6.2	Технология защиты речевой информации в помещениях /Пр/	6	6	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	Работа в группе, решение практико-ориентированных задач
6.3	Обнаружение передающих устройств /Лаб/	6	8	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
6.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	6	36	ОПК-7	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Э1 Э2 Э3	
	Раздел 7. Задачи технической защиты информации. Принципы технической защиты информации. Основные методы защиты информации техническими средствами					
7.1	Задачи технической защиты информации. принципы технической защиты информации. Основные методы защиты информации техническими средствами. Способы и средства инженерной защиты и технической охраны объектов. Подсистема инженерной защиты. /Лек/	6	4	ОПК-7	Л1.1Л2.2 Э1 Э2 Э3	
7.2	Технология защиты речевой информации в помещениях /Пр/	6	4	ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л2.2Л3.2 Э1 Э2 Э3	
7.3	Проведение специальных исследований технических средств и контроля защищенности объектов информатизации /Лаб/	6	10	ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13	Л2.2Л3.1 Э1 Э2 Э3	Моделирование конкретных ситуаций
7.4	Изучение основной и дополнительной литературы по тематике раздела /Ср/	6	36	ОПК-7	Л1.1Л2.2 Л2.3 Л2.4 Л2.5 Л2.6 Л2.7 Л2.8 Л2.9 Л2.10 Л2.11 Л2.12 Л2.13 Л2.14 Л2.15 Э1 Э2 Э3	
7.5	Промежуточная аттестация /Экзамен/	6	36	ОПК-7 ПК-1 ПК-4 ПК-5 ПК-6 ПК-11 ПК-12 ПК-13 ПК-15	Л1.1Л2.2Л3.1 Л3.2 Л3.3 Э1 Э2 Э3	

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	Черенев Ю. Б.	Техническая защита информации: 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	Грибунин В. Г., Чудовский В. В.	Комплексная система защиты информации на предприятии: учебное пособие для студентов вузов, обучающихся по специальностям "Организация и технология защиты информации", "Комплексная защита объектов информатизации"	Москва: Академия, 2009	
Л2.3		Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_61798/
Л2.4		ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения: официальное издание	Москва: Стандартинформ, 2007	http://gostexpert.ru/gost/gost-51275-2006#text
Л2.5		Положение о постоянно действующей технической комиссии (ПДТК) по защите государственной тайны (ДСП)	Приказ Гостехкомиссии России и ФСБ России от 28.07.2001 г. №309/405	
Л2.6		Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам (ДСП)	Утв. Гостехкомиссией России 08.11.2001 г.	
Л2.7		Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и(или) передачи по линиям связи конфиденциальной информации (ДСП)	Утв. Гостехкомиссией России 08.11.2001 г.	

Л2.8		Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации (ДСП)	Утв. Гостехкомиссией России 08.11.2001 г.	
Л2.9		Указ Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" (с изменениями и дополнениями)		http://www.consultant.ru/document/cons_doc_LAW_13532/
Л2.10		Защита информации. Инсайд: специализированное отечественное периодическое издание	Издательский Дом «Афина»	https://elibrary.ru/title_about.asp?id=25917
Л2.11		Вестник УрФО. Безопасность в информационной сфере: специализированное отечественное периодическое издание	Изд-во ЮУрГУ	https://elibrary.ru/title_about.asp?id=32751
Л2.12		Безопасность информационных технологий: специализированное отечественное периодическое издание	Изд-во Национального исследовательского ядерного университета «МИФИ»	https://elibrary.ru/title_about.asp?id=8429
Л2.13		Information and Computer Security: специализированное зарубежное периодическое издание	Emerald	https://www.scopus.com/sourceid/21100421900?origin=resultslist
Л2.14		Information Security Journal: специализированное зарубежное периодическое издание	Taylor & Francis	https://www.scopus.com/sourceid/19700187807?origin=resultslist
Л2.15		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	Черенев Ю. Б.	Техническая защита информации: методические рекомендации к лабораторным работам 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
Л3.2	Паршин К. А.	Технология защиты речевой информации в помещениях: учебно-методическое пособие по дисциплине «Техническая защита информации» 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	Паршин К. А.	Техническая защита информации: методические указания к выполнению курсового проекта для студентов очной формы обучения 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	Официальный сайт Федеральной службы по техническому и экспортному контролю (Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)
Э2	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)
Э3	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.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 Гаран
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	Банк данных угроз безопасности информации ФСТЭК России: https://bdu.fstec.ru/
6.3.2.6	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 "Технологии обеспечения информационной безопасности и техническая защита информации" - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	Специализированная мебель Лабораторное оборудование: Анализатор качества электроэнергии в трехфазных сетях FLUKE 435 Анализатор спектра портативный R&S FSH 4/8 Комплекс программно-аппаратный Oscor-5000 Всенаправленный источник звука Bruel&Kjaer 4296 Генератор шума "ГРОМ-ЗИ-4" Детектор звукозаписывающих устройств Имитатор электростатических разрядов ЭСР-8000 К Индикатор поля D-008 Подавитель сотовой связи ЛГШ-718 Тестер кабельный MicroScanner2 Универсальный анализатор проводных линий ULAN-2 Шумомер-виброметр, анализатор спектра портативный ОКТАВА-110А с антеннами измерительными Система автоматизированная измерения действующих высот случайных антенн и коэффициентов реального затухания электромагнитных сигналов СТЕНТОР-М1 Комплекс для проведения акустических и виброакустических измерений "Спрут-7А" Оборудование для центра защиты информации, включающее комплекс виброакустической защиты "Барон", поисковый прибор "ОРИОН", измеритель параметров проводных коммуникаций LBD-50, прибор блокирования сотовых телефонов "Скат"
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	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

(занятий семинарского типа) и лабораторных занятий, групповых и индивидуальных консультаций	Технические средства обучения - Комплект мультимедийного оборудования
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
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).