ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

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

Б1.В.03 Управление информационной безопасностью на объектах транспортной инфраструктуры

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) **4 ЗЕТ**

Часов по учебному плану 144
в том числе:
аудиторные занятия 54
самостоятельная работа 54
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	54	54	54	54
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Изучение основных понятий, методологии и практических приемов управления технической и организационной инфраструктурой обеспечения информационной безопасности на предприятии.
1.2	Приобретение обучаемыми необходимого объема знаний и практических навыков в области управления информационной безопасностью в системах критической информационной инфраструктуры.
1.3	Формирование у обучаемых целостного представления об организации и содержании процессов управления информационной безопасностью на предприятии как результата внедрения системного подхода к решению задач обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОП	
Цикл (раздел) ОП:	Б1.В

2.1 Требования к предварительной подготовке обучающегося:

Для изучения данной учебной дисциплины необходимы знания, умения и навыки, приобретенные в ходе изучения дисциплин Организационное и правовое обеспечение информационной безопасности, Теория информационной безопасности и методология защиты информации.
В результате освоения предшествующих дисциплин обучающийся должен знать: основы российской правовой системы и законодательства; основные понятия и методы в управленческой деятельности; место и роль информационной безопасности в системе национальной безопасности Российской Федерации; методологию создания систем защиты информации;
уметь: использовать в практической деятельности правовые знания; оценивать эффективность управленческих решений; анализировать и оценивать угрозы информационной безопасности объекта; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; 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;
владеть: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками обоснования, выбора, реализации и контроля результатов управленческого решения; профессиональными способами обеспечения безопасности в сфере информации; профессиональной терминологией в области информационной безопасности.

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-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 защиты

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-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-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	методы управления информационной безопасностью
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовывать работу по управлению информационной безопасностью
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	навыками участия в экспертизе состояния защищенности информации на объекте защиты

ПСК-2: способностью принимать участие в эксплуатации подсистем управления информационной безопасностью предприятия	
Знать:	
Уровень 1	основные методы управления информационной безопасностью
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	выявлять уязвимости информационно-технологических ресурсов информационных систем, проводить мониторинг угроз безопасности информационных систем
Уровень 2	определять комплекс мер для обеспечения информационной безопасности информационных систем
Уровень 3	контролировать эффективность принятых мер по обеспечению информационной безопасности
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

ПСК-3: способностью участвовать в разработке подсистемы управления информационной безопасностью	
Знать:	
Уровень 1	основные методы управления информационной безопасностью
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

ПСК-5: способностью разрабатывать предложения по совершенствованию системы управления информационной безопасностью	
Знать:	
Уровень 1	методологию создания систем защиты информации
Уровень 2	современные подходы к построению систем защиты информации
Уровень 3	перспективные направления развития средств и методов защиты информации
Уметь:	
Уровень 1	пользоваться современной научно-технической информацией по исследуемым задачам
Уровень 2	применять нормативные правовые акты и нормативные методические документы в области обеспечения информационной безопасности
Уровень 3	разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации
Владеть:	
Уровень 1	навыками анализа информационной инфраструктуры информационной системы и ее безопасности
Уровень 2	методами формирования требований по защите информации
Уровень 3	методами мониторинга и аудита, выявления угроз информационной безопасности

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

Уровень 1	основные методы управления информационной безопасностью
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;
3.1.2	принципы организации информационных систем в соответствии с требованиями по защите информации в системах критической информационной инфраструктуры;
3.1.3	основные нормативные правовые акты в области информационной безопасности и защиты информации в системах критической информационной инфраструктуры.
3.2	**Уметь:**
3.2.1	анализировать и оценивать угрозы информационной безопасности объекта;
3.2.2	применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем;
3.2.3	пользоваться нормативными документами по защите информации;
3.2.4	формулировать и настраивать политику безопасности распространенных операционных систем, а также вычислительных сетей, построенных на их основе.
3.3	**Владеть:**
3.3.1	навыками работы с нормативными правовыми актами;
3.3.2	навыками работы с нормативными документами;
3.3.3	методами и средствами выявления угроз безопасности автоматизированным системам;
3.3.4	методами формирования требований по защите информации;
3.3.5	методами анализа и формализации информационных процессов объекта и связей между ними;
3.3.6	методами организации и управления деятельностью служб защиты информации на предприятии;
3.3.7	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. Теоретические аспекты организации систем управления информационной безопасностью					
1.1	Основные понятия и определения /Лек/	7	2	ПСК-1 ПСК-5 ПСК-6	Л1.1Л2.1 Э1 Э2 Э3	
1.2	Система управления информационной безопасностью /Лек/	7	2	ПСК-1 ПСК-5 ПСК-6	Л1.1Л2.1 Э1 Э2 Э3	
1.3	Политика безопасности /Лек/	7	2	ПСК-1 ПСК-5 ПСК-6	Л1.1Л2.1 Э1 Э2 Э3	
1.4	Организация обеспечения информационной безопасности информационных систем /Лек/	7	4	ПСК-1 ПСК-5 ПСК-6	Л1.1Л2.1 Э1 Э2 Э3	

1.5	Аудит информационной безопасности /Лек/	7	4	ПК-5 ПК-6 ПК-13 ПСК-1 ПСК-5	Л1.1Л2.1 Э1 Э2 Э3	
1.6	Средства поддержки процессов управления информационной безопасностью /Лек/	7	4	ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6	Л1.1Л2.1 Э1 Э2 Э3	
1.7	Изучение основной и дополнительной литературы, нормативных правовых и нормативных методических документов /Ср/	7	18	ПК-5 ПК-6 ПК-13 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6	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 Л3.1 Э1 Э2 Э3	
	Раздел 2. Системы управления информационной безопасностью в АСУ ТП на КВО					
2.1	Элементы разработки систем управления информационной безопасностью в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, в том числе на объектах транспортной инфраструктуры /Пр/	7	36	ПК-5 ПК-6 ПК-13 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6 ПК-14	Л2.1Л3.2 Э2 Э3 Э4	Групповая дискуссия
2.2	Изучение основной и дополнительной литературы, нормативных правовых и нормативных методических документов /Ср/	7	36	ПК-5 ПК-6 ПК-13 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6	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 Л3.1 Э1 Э2 Э3 Э4	
2.3	Промежуточная аттестация /Экзамен/	7	36	ПК-5 ПК-6 ПК-13 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6 ПК-14	Л1.1Л2.1Л3.1 Э1 Э2 Э3 Э4	

5. ФОНД ОЦЕНОЧНЫХ МАТЕРИАЛОВ

Фонд оценочных материалов по дисциплине, состоящий из ФОМ для текущего контроля и проведения промежуточной аттестации обучающихся, разрабатывается по каждой дисциплине и хранится на кафедре. Оценочные материалы дублируются на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), доступной через личный кабинет обучающегося.

Фонд оценочных материалов для проведения промежуточной аттестации обучающихся по дисциплине (модулю), включая порядок проведения промежуточной аттестации, систему оценивания результатов промежуточной аттестации и критерии выставления оценок, примеры типовых заданий или иных материалов, необходимых для оценки знаний, умений, навыков, используемых для промежуточной аттестации по дисциплине, приведен в приложении 1 к рабочей программе дисциплины.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1.1. Основная учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка

Л1.1	Зырянова Т. Ю., Паршин К. А.	Управление информационной безопасностью на объектах транспортной инфраструктуры: 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	Милославская Н. Г.	"Серия «Вопросы управление информационной безопасностью"". Выпуск 3"	Москва: Горячая линия-Телеком, 2013	https://e.lanbook.com/book/5180
Л2.2		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/
Л2.3		ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология: официальное издание	Москва: Стандартинформ, 2014	http://gostexpert.ru/gost/gost-27000-2012#text
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)	Приказ ФСТЭК России от 14.03.2014 г. №31	http://www.consultant.ru/document/Cons_doc_LAW_165503/
Л2.5		Приказ Федеральной службы по техническому и экспортному контролю от 23 марта 2017 г. N 49 "О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21, и в Требования 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..."	Приказ ФСТЭК от 23.03.2017 г. №49	http://www.consultant.ru/document/cons_doc_LAW_215942/
Л2.6		Общие требования по обеспечению информационной безопасности в ключевых системах информационной инфраструктуры (ДСП)	Утв. ФСТЭК России 18.05.2007 г.	

Л2.7		Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (ДСП)	Утв. ФСТЭК России 19.11.2007 г.	
Л2.8		Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (ДСП)	Утв. ФСТЭК России 18.05.2007 г.	
Л2.9		Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (ДСП)	Утв. ФСТЭК России 18.05.2007 г.	
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	Зырянова Т. Ю.	Управление информационной безопасностью на объектах транспортной инфраструктуры: методические рекомендации по организации самостоятельной работы по дисциплине «Управление информационной безопасностью на объектах транспортной инфраструктуры» 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.	Управление информационной безопасностью на объектах транспортной инфраструктуры: методические рекомендации к практическим занятиям по дисциплине «Управление информационной безопасностью на объектах транспортной инфраструктуры» 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	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)
Э2	Система электронной поддержки обучения Blackboard Learn (http:// bb.usurt.ru)
Э3	Официальный сайт Федеральной службы по техническому и экспортному контролю Российской Федерации
Э4	Официальный сайт ОАО "Российские железные дороги" (http://www.pzd.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	ГОСТ Эксперт - единая база ГОСТов Российской Федерации
6.3.2.4	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
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
Кабинет "Управление информационной безопасностью". Компьютерный класс - Учебная аудитория для проведения практических (занятий семинарского типа) и лабораторных занятий	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 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
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).