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-2021.plx
10.03.01 Информационная безопасность

Направленность (профиль) Организация и технологии 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 36
часов на контроль 36

Промежуточная аттестация и формы контроля:
экзамен 7

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

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РП	УП	РП
Лекции	18	18	18	18
Практические	36	36	36	36
Элект	18	18	18	18
Итого ауд.	54	54	54	54
Контактная работа	72	72	72	72
Сам. работа	36	36	36	36
Часы на контроль	36	36	36	36
Итого	144	144	144	144

1. ЦЕЛЬ И ЗАДАЧИ 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)
Производственная практика (преддипломная практика)

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
ПК-3: Способен устанавливать и настраивать средства защиты информации в автоматизированных системах
ПК-3.3: Знает основные меры по защите информации в автоматизированных системах
ПК-3.2: Владеет навыками установки и настройки средств защиты информации в автоматизированных системах
ПК-3.1: Знает основные угрозы безопасности информации и модели нарушителя в автоматизированных системах
ПК-4: Способен проводить работы по техническому обслуживанию защищенных технических средств защиты информации
ПК-4.3: Выполняет техническое обслуживание технических средств обработки информации в защищенном исполнении
ПК-4.2: Знает порядок аттестации объектов информатизации на соответствие требованиям безопасности информации
ПК-4.1: Знает проектную документацию на систему защиты объекта информатизации
ПК-5: Способен проводить мониторинг защищенности информации в автоматизированных системах
ПК-5.3: Анализирует недостатки в функционировании системы защиты информации автоматизированной системы
ПК-5.4: Применяет технические средства контроля эффективности средств защиты информации
ПК-5.1: Проводит мониторинг угроз безопасности информации в автоматизированных системах
ПК-5.2: Принимает меры защиты информации при выявлении новых угроз безопасности информации
ПК-6: Способен разрабатывать организационно-распорядительные документы по защите информации в автоматизированных системах
ПК-6.1: Применяет руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации

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. Введение в управление информационной безопасностью на объектах транспортной инфраструктуры					
1.1	Основы, термины, определения /Лек/	7	2	ПК-6.1	Л1.1Л2.1 Э2 Э3 Э4	
1.2	Субъекты информационных отношений на объектах транспортной инфраструктуры /Пр/	7	4	ПК-6.1	Л1.1Л2.1Л3.2 Э2 Э3 Э4	Работа в группе. Групповая дискуссия
1.3	Нормативные правовые акты Российской Федерации в области обеспечения информаицонной безопасности объектов транспортной инфраструктуры /Лек/	7	2	ПК-6.1	Л1.1Л2.1 Э2 Э3 Э4	
1.4	Порядок вступления в силу нормативных правовых актов /Пр/	7	4	ПК-6.1	Л1.1Л2.1Л3.2 Э2 Э3 Э4	Работа в группе. Групповая дискуссия
1.5	Требования к системам защиты информации на объектах транспортной инфраструктуры /Лек/	7	2	ПК-6.1	Л1.1Л2.1 Э2 Э3 Э4	
1.6	Принятие решения о создании системы управления информационной безопасностью /Пр/	7	4	ПК-6.1	Л1.1Л2.1Л3.2 Э2 Э3 Э4	Работа в группе. Групповая дискуссия
1.7	Изучение литературы и нормативных правовых документов по тематике раздела. Подготовка отчетов по практическим занятиям /Ср/	7	12	ПК-6.1	Л1.1Л2.1Л3.1 Л3.2 Э2 Э3 Э4	
	Раздел 2. Угрозы безопасности информации на объектах транспортной инфрастукруры					

2.1	Определение угроз безопасности информации на объектах транспортной инфраструктуры /Лек/	7	4	ПК-3.1 ПК-5.1 ПК-5.3	Л1.1Л2.1 Э2 Э3 Э4	
2.2	Определение актуальных угроз безопасности информации на объектах транспортной инфраструктуры /Лек/	7	2	ПК-3.1 ПК-5.1 ПК-5.3	Л1.1Л2.1 Э2 Э3 Э4	
2.3	Построение модели угроз безопасности информации для объекта транспортной инфраструктуры /Пр/	7	12	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1Л3.2 Э2 Э3 Э4	Работа в группе. Построение модели по заданной методике
2.4	Изучение литературы и нормативных правовых документов по тематике раздела. Подготовка отчетов по практическим занятиям /Ср/	7	12	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1Л3.1 Л3.2 Э2 Э3 Э4	
	Раздел 3. Стандартизация в области управления информационной безопасностью на объектах транспортной инфраструктуры					
3.1	Обзор стандартов управления информационной безопасностью /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-5.1 ПК-5.3 ПК-6.1	Л1.1Л2.1 Э1 Э2 Э3 Э4	
3.2	Критерии оценки безопасности информационных технологий на объектах транспортной инфраструктуры /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-5.1 ПК-5.3 ПК-6.1	Л1.1Л2.1 Э1 Э2 Э3 Э4	
3.3	Профили защиты средств защиты информации на объектах транспортной инфраструктуры /Лек/	7	2	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-5.1 ПК-5.3 ПК-6.1	Л1.1Л2.1 Э1 Э2 Э3 Э4	
3.4	Анализ стандартов управления информационной безопасностью /Пр/	7	12	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-5.1 ПК-5.3 ПК-6.1	Л1.1Л2.1Л3.2 Э1 Э2 Э3 Э4	Работа в группе. проведение анализа по заданной методике
3.5	Изучение литературы и нормативных правовых документов по тематике раздела. Подготовка отчетов по практическим занятиям /Ср/	7	12	ПК-3.1 ПК-3.3 ПК-4.1 ПК-4.2 ПК-5.1 ПК-5.3 ПК-6.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	
3.6	Взаимодействие с обучающимися по вопросам текущего контроля в электронной информационно-образовательной среде: выполнение контрольных заданий и промежуточных тестов /Элект/	7	18	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1Л3.1 Л3.2 Э1 Э2 Э3 Э4	

3.7	Промежуточная аттестация /Экзамен/	7	36	ПК-3.1 ПК-3.2 ПК-3.3 ПК-4.1 ПК-4.2 ПК-4.3 ПК-5.1 ПК-5.2 ПК-5.3 ПК-5.4 ПК-6.1	Л1.1Л2.1Л3.1 Л3.2 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

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	http://e.lanbook.com

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
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

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
Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа (практических занятий, лабораторных занятий), курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также для самостоятельной работы. Специализированный кабинет «Управление информационной безопасностью».	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. Обучающемуся 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 обучающихся 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. Для закрепления теоретического материала в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru) размещены тестовые материалы. Число тренировочных попыток ограничено. Тестовые материалы сформированы в логической последовательности в соответствии с изученными темами. Совместная деятельность преподавателя и обучающихся по проверке выполнения мероприятий текущего контроля, предусмотренных рабочей программой дисциплины (модуля) организована в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru). Для корректной работы в системе обучающиеся в разделе "Личные сведения" должны ввести актуальный адрес своей электронной почты. Формы самостоятельной работы обучающихся по данной дисциплине разнообразны. Они включают в себя:- изучение теоретического материала (учебной, научной, методической литературы, материалов периодических изданий);- подготовку к занятиям, предусмотренным РПД, мероприятиям текущего контроля, промежуточной аттестации и т.д. Выполнять самостоятельную работу и отчитываться по ее результатам обучающийся должен в соответствии с календарным планом изучения дисциплины, видами и сроками отчетности. При выполнении самостоятельной работы обучающемуся рекомендуется руководствоваться учебно-методическими материалами, размещенными на странице данного курса в системе электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru), а также учебно-методическими материалами, которые указаны для самостоятельной работы по темам дисциплины в разделе 4 РПД "Структура и содержание дисциплины (модуля)".Перечень учебно-методических материалов (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).
При применении дистанционных образовательных технологий и электронного обучения освоение дисциплины (модуля) осуществляется в электронно-информационной образовательной среде (образовательная платформа электронной поддержки обучения Blackboard Learn (сайт bb.usurt.ru)) в рамках созданного курса, что позволяет реализовывать асинхронное и синхронное взаимодействие участников образовательных отношений.