Приложение 5

ПРОГРАММЫ ПРАКТИК

По направлению подготовки
10.03.01 «Информационная безопасность**»**

Направленность (профиль)
«Организация и технология защиты информации (на транспорте)**»**

Форма обучения
«Очная»

Б2.В.01(У) Учебная практика (практика по получению первичных профессиональных умений и навыков)…… ……..2

Б2.В.02(У) Учебная практика (ознакомительная практика)……. 10

Б2.В.03(У) Учебная практика (технологическая практика)…….. 19

Б2.В.04(П) Производственная практика (проектно-технологическая практика)……..... 29

Б2.В.05(П) Производственная практика (эксплуатационная практика)…… ……42

Б2.В.06(Пд) Преддипломная практика……..54

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.01(У) Учебная практика (практика по получению первичных профессиональных умений и навыков)

программа практики

Закреплена за кафедрой Информационные технологии и защита информации

Учебный план 10.03.01 ИБ 3+ 2018.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Специализация

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **1 ЗЕТ**

Способ проведения Стационарный, выездной

Форма проведения Дискретная

Часов по учебному плану 36
в том числе:
аудиторные занятия 18
самостоятельная работа 18

Промежуточная аттестация и формы контроля:
зачет с оценкой 6

Часов контактной работы всего, в том числе: 37,8
руководство учебной практикой 18
аудиторная работа 18
текущие консультации по практическим занятиям 1,8

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Практические	18	18	18	18
Итого ауд.	18	18	18	18
Контактная работа	18	18	18	18
Сам. работа	18	18	18	18
Итого	36	36	36	36

Программу составил(и):
старший преподаватель, Гузенкова Е. А.;ассистент, Ганженко Н. В. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В. В. Башуров

Руководитель ОП ВО _____ / Т. Ю. Зырянова

Управление информатизации _____ / А. А. Галочкин

Издательско-библиотечный комплекс _____ / А. А. Колтышев

Учебно-методический отдел _____ / Е. И. Морозова

Отдел производственного обучения и связи с производством _____ / А. Н. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации
ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Кикоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Учебная практика (практика по получению первичных профессиональных умений и навыков)

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: получение первичных профессиональных умений и навыков.
1.2	Задачи практики: научиться проводить анализ защищенности информационных систем предприятия на соответствие нормативным требования законодательства Российской Федерации; получение студентами навыков формирования требований организационно-методического обеспечения защиты информации.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах:
Правовые и экономические аспекты профессиональной деятельности
Физические основы защиты информации
Электротехника, электроника и схемотехника
В результате изучения предыдущих дисциплин и(или) разделов дисциплин у студентов сформированы:
Знания: основные понятия, законы и модели теории колебаний и волн; основные понятия и нормативные, правовые акты информационной безопасности.
Умения: производить математические расчеты по заданным формулам; применять основные законы физики при решении прикладных задач; использовать нормативные документы для обеспечения информационной безопасности.
Владения: методами количественного анализа процессов обработки, поиска и передачи информации; навыками проведения физического эксперимента и обработки его результатов.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Учебная практика (ознакомительная практика)
Учебная практика (технологическая практика)
Производственная практика (проектно-технологическая практика)

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
Знать:	
Уровень 1	основные понятия и определения в области информационной безопасности
Уровень 2	принципы и методы противодействия информационным угрозам
Уровень 3	место и роль информационной безопасности в системе национальной безопасности Российской Федерации
Уметь:	
Уровень 1	выделять актуальные проблемы информационной безопасности
Уровень 2	проводить анализ информационных событий событий, анализировать и оценивать информацию
Уровень 3	планировать и осуществлять свою деятельность с учетом результатов анализа информационных событий
Владеть:	
Уровень 1	навыками самостоятельного решения поставленных задач
Уровень 2	основами построения модели защиты информации
Уровень 3	навыками обоснования выбора направления защиты информации

ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач	
Знать:	
Уровень 1	основы динамики, законы сохранения, механические колебания и волны, основы термодинамики, основы электродинамики
Уровень 2	основные понятия, модели и законы теории колебаний и волн
Уровень 3	особенности физических эффектов и явления, используемых для обеспечения информационной безопасности
Уметь:	
Уровень 1	рассчитывать амплитуду, длину волны, скорость распространения и коэффициент затухания акустической волны, распространяющейся в среде с заданными параметрами
Уровень 2	рассчитывать амплитуду, скорость распространения и длину волны, а также определять вид поляризации поля плоской электромагнитной волны в произвольной среде на заданном расстоянии
Уровень 3	определять углы преломления и отражения плоских акустических и электромагнитных волн на границе раздела двух сред; оценивать акустические и электродинамические параметры произвольной среды на заданной
Владеть:	
Уровень 1	навыками использования программных и аппаратных средств персонального компьютера

Уровень 2	навыками использования справочной литературы
Уровень 3	навыками применения математического аппарата для решения физических задач

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	
Знать:	
Уровень 1	основы математических дисциплин для решения профессиональных задач
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	применять математический аппарат для решения профессиональных задач
Уровень 2	применять криптографические средства, основанные на математических моделях для шифрования информации
Уровень 3	создавать математические модели методов защиты информации посредством применения шифрования
Владеть:	
Уровень 1	математическим аппаратом для решения профессиональных задач
Уровень 2	методологией криптографической защиты информации
Уровень 3	методами создания математических методов защиты информации посредством применения шифрования

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	
Знать:	
Уровень 1	основные законы в области электроники, электротехники и схемотехники
Уровень 2	способы влияния сбора информации посредством передачи электрических сигналов
Уровень 3	методы нанесения ущерба защищаемой информации связанных с устройствами электроники и схемотехники
Уметь:	
Уровень 1	пользоваться документацией, для создания сетевой инфраструктуры и коммутации отдельных компонентов рабочих станций на основе знания схемотехники и электроники
Уровень 2	производить коммутацию сетевого оборудования
Уровень 3	анализировать степень защиты сетевого оборудования при коммутации
Владеть:	
Уровень 1	средствами применения основных законов в области электроники, электротехники и схемотехники
Уровень 2	способами выявления сбора информации посредством передачи электрических сигналов
Уровень 3	методами противодействия нанесению ущерба защищаемой информации

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	
Знать:	
Уровень 1	методики обработки достоверных результатов
Уровень 2	методики оценки достоверных результатов
Уровень 3	способы оценки погрешности
Уметь:	
Уровень 1	проводить эксперименты по заданной методике
Уровень 2	осуществлять оценку полученных результатов
Уровень 3	вычислять погрешность
Владеть:	
Уровень 1	методикой проведения экспериментов
Уровень 2	средствами оценки полученных результатов экспериментов
Уровень 3	методикой вычисления погрешности

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
Знать:	
Уровень 1	основные принципы и закономерности проведения эксперимента по заданной методике
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	принимать участие в проведении экспериментальных исследований системы защиты информации

Уровень 2	формировать заключение по итогам проведения экспериментальных исследований системы защиты информации
Уровень 3	давать экспертную оценку результатам проведения экспериментальных исследований системы защиты информации
Владеть:	
Уровень 1	методикой проведения экспериментальных исследований системы защиты информации
Уровень 2	способами формирования заключения по итогам проведения экспериментальных исследований системы защиты информации
Уровень 3	способами формирования экспертной оценки экспериментальных исследований системы защиты информации

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	методику взаимодействия с коллективом
Уровень 2	способы распределения обязанностей при проведении работ по защите информации
Уровень 3	методику оценки эффективности работы каждого из участников малого коллектива и группы в целом
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	
Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	способы применения математического аппарата в профессиональной деятельности; основные направления информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации; возможные методы и пути реализации угроз защищаемой информации.
3.2	**Уметь:**
3.2.1	находить способы использования основных естественнонаучных законов; использовать программные и аппаратные средства персонального компьютера; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; выявлять угрозы информационной безопасности объекта.
3.3	**Владеть:**
3.3.1	навыками выявления сущности проблем, возникающих в профессиональной деятельности; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; методами формирования требований по защите информации; методами и средствами анализа информационной безопасности объекта.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература
	Раздел 1. Подготовительный этап				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Пр/	6	2	ОК-5 ОПК-1 ОПК-2 ОПК-3 ПК-11 ПК-12 ПК-14	Л1.2 Л2.2 Л3.1 Э1 Э2
1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	6	2	ОК-5	Л1.1 Л1.2 Л1.3 Л2.2 Л3.1 Э1 Э2
	Раздел 2. Изучение нормативных и правовых документов по информационной безопасности				
2.1	Изучение законодательства Российской федерации в области защиты информации /Пр/	6	2	ОК-5 ПК-14	Л1.1 Л2.1 Л3.1 Э1 Э2

2.2	Изучение критериев по безопасности и международных стандартов в сфере информационной безопасности /Пр/	6	2	ОК-5 ОПК-1 ОПК-2 ОПК-3	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
	Раздел 3. Разработка документации по информационной безопасности				
3.1	Методика определения угроз безопасности информации в государственных информационных системах /Пр/	6	2	ОК-5 ОПК-1	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
3.2	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных /Пр/	6	4	ОК-5 ОПК-1	Л1.1 Л2.2 Л3.1 Э1 Э2
3.3	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных /Пр/	6	2	ОК-5 ПК-11 ПК-12	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
3.4	Разработка частной модели угроз безопасности в соотвествии со спецификой предприятия /Пр/	6	4	ОК-5 ПК-11 ПК-12	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
3.5	Изучение литературы и нормативных правовых документов по тематике раздела /Ср/	6	4	ОК-5 ОПК-1	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
	Раздел 4. Разработка документации по информационной безопасности				
4.1	Освоение методов организации и управления деятельности служб защиты информации на предприятии /Ср/	6	2	ОПК-1 ОПК-2 ОПК-3 ПК-14	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
4.2	Изучение литературы и нормативных методических документов по тематике раздела /Ср/	6	2	ОПК-1 ОПК-2 ОПК-3 ПК-11 ПК-12 ПК-14	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
4.3	Выполнение индивидуального задания /Ср/	6	2	ОПК-1 ОПК-2 ОПК-3 ПК-11 ПК-12	Л1.1 Л1.3 Л2.2 Л3.1 Э1 Э2
	Раздел 5. Промежуточная аттестация				
5.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	6	6	ОК-5 ОПК-1 ОПК-2 ОПК-3 ПК-11 ПК-12 ПК-14	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э1 Э2

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	Курило А. П., Милославская Н. Г., Сенаторов М. Ю., Толстой А. И.	Основы управления информационной безопасностью: допущено Учебно-методическим объединением высших учебных заведений России по образованию в области информационной безопасности в качестве учебного пособия для студентов высших учебных заведений, обучающихся по программам бакалавриата, магистратуры и специалитета укрупненного направления 090000 – "Информационная безопасность"	Москва: Горячая линия - Телеком, 2012	http://e.lanbook.com/books/element.php?pl1_id=5178
Л1.2	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.3	Ададуров С. Е., Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: В 2ч.Ч.1: Методология и система обеспечения информационной безопасности на железнодорожном транспорте: Учебник	Москва: ФГБОУ "Учебно-методический центр по образованию на железнодорожном трансторте "(УМЦ ЖДТ), 2014	http://znanium.com/go.php?id=487777

6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2017	http://znanium.com/go.php?id=773209
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688

6.1.3. Методические материалы

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"

Э1	Образовательный контент УрГУПС для обеспечения самостоятельной работы студентов (bb.usurt.ru)
Э2	Сайт Федеральной службы по техническому и экспортному контролю (www.fstec.ru/)

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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	ESET NOD32 Antivirus
6.3.1.4	Adobe Acrobat
6.3.1.5	Справочно-правовая система КонсультантПлюс
6.3.1.6	Система электронной поддержки обучения Blackboard Learn

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант Плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Назначение	Оснащение
Учебная аудитория для проведения текущего контроля и промежуточной аттестации (Компьютерные классы)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
Учебная аудитория для проведения практических занятий (занятий семинарского типа)	Специализированная мебель 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
Учебная аудитория для проведения групповых и индивидуальных консультаций	Специализированная мебель
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

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.02(У) Учебная практика (ознакомительная практика)

программа практики

Закреплена за кафедрой Информационные технологии и защита информации

Учебный план 10.03.01 ИБ 3+ 2018.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Специализация

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **2 ЗЕТ**

Способ проведения Стационарный, выездной

Форма проведения Дискретная

Продолжительность 1,33 недель

Часов по учебному плану	72	Часов контактной работы всего, в том числе:	48
в том числе:		руководство учебной практикой	48
аудиторные занятия	0		
самостоятельная работа	72		

Промежуточная аттестация и формы контроля:
зачет с оценкой 6

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Сам. работа	72	72	72	72
Итого	72	72	72	72

Программу составил(и):
старший преподаватель, Гузенкова Е.А. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В. В. Бакуров

Руководитель ОП ВО _____ / Т. Ю. Гаранина

Управление информатизации _____ / А. А. Балашенцев

Издательско-библиотечный комплекс _____ / А. А. Колтышев

Учебно-методический отдел _____ Е. Н. Морозова

Отдел производственного обучения и связи с производством _____ / А. М. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Кикоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Учебная практика (ознакомительная практика)

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: получение первичных профессиональных умений и навыков.
1.2	Задачи практики: ознакомление студента с организационной структурой предприятия, с его подразделениями; ознакомление студента с нормативными документами, которые являются регламентирующим для предприятия.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах и практиках:
Физические основы защиты информации
Теория информации
Электротехника, электроника и схемотехники
Организационное и правовое обеспечение информационной безопасности
Техническая защита информации
Учебная практика (практика по получению первичных профессиональных умений и навыков)
В результате изучения предыдущих дисциплин и(или) разделов дисциплин, а также практик у студентов сформированы:
Знания: способы применения математического аппарата в профессиональной деятельности; основные направления информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации; возможные методы и пути реализации угроз защищаемой информации.
Умения: находить способы использования основных естественнонаучных законов; использовать программные и аппаратные средства персонального компьютера;
выбирать показатели качества и критерии оценки систем и средств защиты информации;
пользоваться современной научно-технической информацией по вопросам безопасности; выявлять угрозы информационной безопасности объекта.
Владения: навыками выявления сущности проблем, возникающих в профессиональной деятельности; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами;
методами формирования требований по защите информации; методами и средствами анализа информационной безопасности объекта.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Управление информационной безопасностью на объектах транспортной инфраструктуры
Учебная практика (технологическая практика)
Производственная практика (проектно-технологическая практика)
Комплексные системы защиты информации на транспорте

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач	
Знать:	
Уровень 1	основные физические законы в области решения профессиональных задач по обеспечению защиты информации
Уровень 2	способы воздействия физических явлений на безопасность хранения и передачи информации
Уровень 3	способы организации защиты от физических явлений, способных причинить ущерб информации
Уметь:	
Уровень 1	использовать основные законы физики для решения профессиональных задач
Уровень 2	проводить анализ физических явлений, влияющих на безопасность информации
Уровень 3	организовывать защиту от физических явления, влияющих на безопасность информации
Владеть:	
Уровень 1	методами анализа физических явления и процессов для решения профессиональных задач
Уровень 2	методами выявления физических явлений, влияющих на безопасность информации
Уровень 3	методами реализации защиты от физических явлений, влияющих на безопасность информации

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	
Знать:	
Уровень 1	способы применения математического аппарата в профессиональной деятельности
Уровень 2	методы расчета зон безопасности для защиты информации
Уровень 3	совершенствования зон безопасности в существующих предприятиях с учетом специфики обрабатываемой информации
Уметь:	
Уровень 1	находить способы использования основных естественнонаучных законов

Уровень 2	использовать методические рекомендации для расчета зон безопасности
Уровень 3	использовать теорию вероятности возникновения угоз безопасности информации на существующих предприятиях с учетом их специфики
Владеть:	
Уровень 1	навыками выявления сущности проблем, возникающих в профессиональной деятельности
Уровень 2	навыками применения математического аппарата из методических рекомендаций, для расчета зон безопасности
Уровень 3	навыками использования методов вероятностного прогнозирования угроз безопасности на существующих предприятиях

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	
Знать:	
Уровень 1	основные законы в области электроники, электротехники и схемотехники
Уровень 2	способы влияния сбора информации посредством передачи электрических сигналов
Уровень 3	методы нанесения ущерба защищаемой информации связанных с устройствами электроники и схемотехники
Уметь:	
Уровень 1	пользоваться документацией, для создания сетевой инфраструктуры и коммутации отдельных компонентов рабочих станций на основе знания схемотехники и электроники
Уровень 2	производить коммутацию сетевого оборудования
Уровень 3	анализировать степень защиты сетевого оборудования при коммутации
Владеть:	
Уровень 1	способами создания инфраструктуры и коммутации отдельных компонентов рабочих станций на основе знания съемотехники и электроники
Уровень 2	способами коммутации сетевого оборудования
Уровень 3	анализом степени защиты сетевого оборудования при коммутации

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Знать:	
Уровень 1	основы организационного и правового обеспечения информационной безопасности
Уровень 2	нормативные методические документы ФСБ России и ФСТЭК России в области защиты объекта информатизации
Уровень 3	нормативные документы по безопасности, разработанные в организации
Уметь:	
Уровень 1	осуществлять правовую оценку объекта информатизации;
Уровень 2	применять нормативные правовые акты и нормативные методические документы в области информационной безопасности
Уровень 3	производить анализ информационной безопасности объекта
Владеть:	
Уровень 1	методами осуществления правовой оценки объекта
Уровень 2	способами применения правовых актов и нормативных методических документов в области информационной безопасности
Уровень 3	способами проведения анализа информационной безопасности объекта

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	методику организации контрольных проверок работоспособности программно-аппаратных средств защиты информации
Уровень 2	методику проведения контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	нормативные документы, посредством которых организуется проведение контрольных проверок применяемых средств защиты информации
Уметь:	
Уровень 1	использовать методику контрольных проверок работоспособности и эффективности программных средств защиты информации
Уровень 2	использовать методику контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	использовать методику контрольных проверок работоспособности и эффективности технических средств

	защиты информации
Владеть:	
Уровень 1	методами анализа работоспособности и эффективности программных средств защиты информации
Уровень 2	методами анализа работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	методами анализа работоспособности и эффективности технических средств защиты информации

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	методику взаимодействия с коллективом
Уровень 2	способы распределения обязанностей при проведении работ по защите информации
Уровень 3	методику оценки эффективности работы каждого из участников малого коллектива и группы в целом
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	
Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	способы применения математического аппарата в профессиональной деятельности; основные направления информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации; возможные методы и пути реализации угроз защищаемой информации
3.2	**Уметь:**
3.2.1	находить способы использования основных естественнонаучных законов; использовать программные и аппаратные средства персонального компьютера; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; выявлять угрозы информационной безопасности объекта
3.3	**Владеть:**
3.3.1	навыками выявления сущности проблем, возникающих в профессиональной деятельности; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; методами формирования требований по защите информации; методами и средствами анализа информационной безопасности объекта

4. СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература
	Раздел 1. Изучение инструктажей				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Ср/	6	2	ПК-14	Л1.5 Л2.2 Л3.1 Э5
1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	6	2	ОПК-1 ОПК-2 ОПК-3 ПК-5 ПК-6 ПК-14	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э2 Э3 Э4 Э5
	Раздел 2. Изучение документации по информационной безопасности на предприятии				
2.1	Организационная структура предприятия. Функции отделов и служб, Технология работы объекта практики, нормативные акты предприятия. Информационные средства и информационные системы по защите информации. /Ср/	6	18	ОПК-1 ОПК-2 ПК-5 ПК-6 ПК-14	Л1.2 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э5

2.2	Изучение, систематизация, анализ и сбор материала для формирования отчета по практике; Формирование отчета о прохождении практики, включая выполнение индивидуального задания; Ведение студенческой аттестационной книжки, включая получение отзыва руководителя предприятия /Ср/	6	42	ОПК-1 ОПК-2 ОПК-3 ПК-5 ПК-6	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Промежуточная аттестация				
3.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	6	8	ОПК-1 ОПК-2 ОПК-3 ПК-5 ПК-6	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	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	
Л1.2	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальности "Информационная безопасность"	Москва: Академия, 2009	
Л1.3	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	
Л1.4	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	http://e.lanbook.com/books/element.php?pl1_id=59241

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.5	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.6	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644

6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Рос. НИИ и проектно-конструкторский ин-т информатизации, автоматизации и связи, Отделение информации (ЦНИИТЭИ)	Указатель документов, действующих в ОАО "РЖД": указатель	Москва, 2004	
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688
Л2.3	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=927768

6.1.3. Методические материалы

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"

Э1	Консультант Плюс (http://www.consultant.ru)
Э2	Федеральная служба по техническому и экспортному контролю (https://fstec.ru/)
Э3	Федеральная служба безопасности Российской Федерации (http://www.fsb.ru/)
Э4	Система электронной поддержки обучения Blackboard Learn (https://bb.usurt.ru/)
Э5	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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	Операционная система Astra Linux
6.3.1.4	ESET NOD32 Antivirus
6.3.1.5	Платформа управления базами данных: SQL Server
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Abbyy FineReader
6.3.1.8	Adobe Acrobat
6.3.1.9	Система электронной поддержки обучения Blackboard Learn
6.3.1.10	Secret Net Studio
6.3.1.11	Система защиты информации от несанкционированного доступа: Dallas Lock

6.3.1.12	Linux Debian
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант Плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Назначение	Оснащение
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, 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
База практики (Материальная техническая база профильной организации)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети Интернет Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях для конкретных видов работ
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
Учебная аудитория для проведения текущего контроля и промежуточной аттестации	Специализированная мебель

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.03(У) Учебная практика (технологическая практика)

программа практики

Закреплена за кафедрой Информационные технологии и защита информации

Учебный план 10.03.01 ИБ 3+ 2018.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Специализация

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **3 ЗЕТ**

Способ проведения Стационарный, выездной

Форма проведения Дискретная

Продолжительность 2 недель

Часов по учебному плану	108	Часов контактной работы всего, в том числе:	72
в том числе:		руководство учебной практикой	72
аудиторные занятия	0		
самостоятельная работа	108		

Промежуточная аттестация и формы контроля:
зачет с оценкой 6

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**6 (3.2)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Сам. работа	108	108	108	108
Итого	108	108	108	108

Программу составил(и):
старший преподаватель, Гузенкова Е.А. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В. В. Бакуров

Руководитель ОП ВО _____ / Т. Ю. Зырянова

Управление информатизации _____ / А. А. Толочинцев

Издательско-библиотечный комплекс _____ / А. А. Колтачев

Учебно-методический отдел _____ / Е. Н. Морозова

Отдел производственного обучения и связи с производством _____ / А. Н. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Кикоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Учебная практика (технологическая практика)

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: получение первичных профессиональных умений и навыков
1.2	Задача практики: конфигурирование используемых на объектах практики программных и технических средств защиты информации.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах и практиках:
Иностранный язык
Русский язык и этика делового общения
Социальные и психологические аспекты профессиональной деятельности
Физические основы защиты информации
Электротехника, электроника и схемотехника
Правовые и экономические аспекты профессиональной деятельности
Организационное и правовое обеспечение информационной безопасности
Техническая защита информации
Безопасность информационных процессов
Безопасность сетей ЭВМ
Стеганография
Теория информационной безопасности и методология защиты информации
Учебная практика (ознакомительная практика)
Учебная практика (практика по получению первичных профессиональных умений и навыков)
В результате изучения предыдущих дисциплин и(или) разделов дисциплин, а также практик у студентов сформированы:
Знания: способы применения математического аппарата в профессиональной деятельности; основные направления информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации; возможные методы и пути реализации угроз защищаемой информации.
Умения: выбирать показатели качества и критерии оценки систем и средств защиты информации;
пользоваться современной научно-технической информацией по вопросам безопасности; выявлять угрозы информационной безопасности объекта.
Владения: навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности;
навыками работы с нормативными правовыми актами;
методами формирования требований по защите информации; методами и средствами анализа информационной безопасности объекта.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Программно-аппаратные средства защиты информации
Основы управления информационной безопасностью
Производственная практика (проектно-технологическая практика)
Государственная итоговая аттестация
Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОК-5: способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	
Знать:	
Уровень 1	место информационной безопасности в системе национальной безопасности Российской Федерации
Уровень 2	роль информационной безопасности в системе национальной безопасности Российской Федерации
Уровень 3	место и роль международной информационной безопасности
Уметь:	
Уровень 1	выделять актуальные проблемы информационной безопасности
Уровень 2	сопоставлять актуальные проблемы информационной безопасности с проблемами по информационной безопасности Российской Федерации
Уровень 3	сопоставлять актуальные проблемы информационной безопасности с проблемами международной информационной безопасности
Владеть:	
Уровень 1	основами построения модели нарушителя
Уровень 2	основами построения модели актуальных угроз
Уровень 3	основами построения модели защиты информации

ОК-7: способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности	
Знать:	
Уровень 1	грамматику русского языка
Уровень 2	грамматику иностранного языка
Уровень 3	специфику решения задач межличностного и межкультурного взаимодействия
Уметь:	
Уровень 1	грамотно обосновывать решения в области своей профессиональной деятельности
Уровень 2	грамотно и с применением профессиональных терминов выдавать решения в области своей профессиональной деятельности в устной и письменной формах на русском языке
Уровень 3	грамотно и с применением профессиональных терминов выдавать решения в области своей профессиональной деятельности в устной и письменной формах на русском языке
Владеть:	
Уровень 1	способностью к коммуникации в письменной форме на русском языке для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности
Уровень 2	способностью к коммуникации в устной форме на русском языке для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности
Уровень 3	способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности

ОК-8: способностью к самоорганизации и самообразованию	
Знать:	
Уровень 1	методику организации самостоятельного изучения материалов практики
Уровень 2	способы самоорганизации
Уровень 3	способы самообразования
Уметь:	
Уровень 1	организовать самостоятельную работу с источниками информации
Уровень 2	организовывать самостоятельную работу с иностранными источниками информации
Уровень 3	проводить самостоятельно анализ собранной информации и делать выводы, по полученным результатам
Владеть:	
Уровень 1	методикой организации самостоятельного изучения материалов практики
Уровень 2	способами сбора, обработки и переработки собранной, во время практики, информации
Уровень 3	эффективным анализом полученной во время практики информации для формирования выводов по проделанной работы

ОПК-1: способностью анализировать физические явления и процессы для решения профессиональных задач	
Знать:	
Уровень 1	основные физические законы в области решения профессиональных задач по обеспечению защиты информации
Уровень 2	способы воздействия физических явлений на безопасность хранения и передачи информации
Уровень 3	способы организации защиты от физических явлений, способных причинить ущерб информации
Уметь:	
Уровень 1	использовать основные законы физики для решения профессиональных задач
Уровень 2	проводить анализ физических явлений, влияющих на безопасность информации
Уровень 3	организовывать защиту от физических явления, влияющих на безопасность информации
Владеть:	
Уровень 1	методами анализа физических явления и процессов для решения профессиональных задач
Уровень 2	методами выявления физических явлений, влияющих на безопасность информации
Уровень 3	методами реализации защиты от физических явлений, влияющих на безопасность информации

ОПК-2: способностью применять соответствующий математический аппарат для решения профессиональных задач	
Знать:	
Уровень 1	способы применения математического аппарата в профессиональной деятельности
Уровень 2	методы расчета зон безопасности для защиты информации
Уровень 3	совершенствования зон безопасности в существующих предприятиях с учетом специфики обрабатываемой информации
Уметь:	

Уровень 1	находить способы использования основных естественнонаучных законов
Уровень 2	использовать методические рекомендации для расчета зон безопасности
Уровень 3	использовать теорию вероятности возникновения угоз безопасности информации на существующих предприятиях с учетом их специфики
Владеть:	
Уровень 1	навыками выявления сущности проблем, возникающих в профессиональной деятельности
Уровень 2	навыками применения математического аппарата из методических рекомендаций, для расчета зон безопасности
Уровень 3	навыками использования методов вероятностного прогнозирования угроз безопасности на существующих предприятиях

ОПК-3: способностью применять положения электротехники, электроники и схемотехники для решения профессиональных задач	
Знать:	
Уровень 1	основные законы в области электроники, электротехники и схемотехники
Уровень 2	способы влияния сбора информации посредством передачи электрических сигналов
Уровень 3	методы нанесения ущерба защищаемой информации связанных с устройствами электроники и схемотехники
Уметь:	
Уровень 1	пользоваться документацией, для создания сетевой инфраструктуры и коммутации отдельных компонентов рабочих станций на основе знания схемотехники и электроники
Уровень 2	производить коммутацию сетевого оборудования
Уровень 3	анализировать степень защиты сетевого оборудования при коммутации
Владеть:	
Уровень 1	средствами применения основных законов в области электроники, электротехники и схемотехники
Уровень 2	способами выявления сбора информации посредством передачи электрических сигналов
Уровень 3	методами противодействия нанесению ущерба защищаемой информации

ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
Знать:	
Уровень 1	значение информации в развитии современного общества
Уровень 2	средства сбора, обработки и хранения информации
Уровень 3	способы поиска и обработки информации
Уметь:	
Уровень 1	использовать программные и аппаратные средства персонального компьютера
Уровень 2	выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности
Уровень 3	пользоваться современной научно-технической информацией по вопросам безопасности
Владеть:	
Уровень 1	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
Уровень 2	навыками работы с нормативными правовыми актами
Уровень 3	методами формирования требований по защите информации

ОПК-5: способностью использовать нормативные правовые акты в профессиональной деятельности	
Знать:	
Уровень 1	основы организационного и правового обеспечения информационной безопасности
Уровень 2	нормативные методические документы ФСБ России и ФСТЭК России в области защиты информации
Уровень 3	международные стандарты в области защиты информации
Уметь:	
Уровень 1	осуществлять правовую оценку информации
Уровень 2	применять нормативные правовые акты и нормативные методические документы в области информационной безопасности
Уровень 3	использовать международные стандарты для защиты информации
Владеть:	
Уровень 1	основами организационного и правового обеспечения информационной безопасности
Уровень 2	методикой формирования политики безопасности в организации на основе нормативных и правовых актов органов регуляторов в сфере информационной безопасности
Уровень 3	методикой формирования политики безопасности организации на основе международных стандартов по

	защите информации

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	определять информационные ресурсы, подлежащие защите
Уровень 2	выявлять угрозы информационной безопасности объекта
Уровень 3	на основе выявленных угроз безопасности объекта выбирать актуальные угрозы
Владеть:	
Уровень 1	способами классификации защищаемой информации на исследуемом объекте
Уровень 2	способами классификации угроз информации на исследуемом объекте
Уровень 3	средствами, методами и способами реализации защитных мер от угроз защищаемой информации на исследуемом объекте

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	методику взаимодействия с коллективом
Уровень 2	способы распределения обязанностей при проведении работ по защите информации
Уровень 3	методику оценки эффективности работы каждого из участников малого коллектива и группы в целом
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	
Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

В результате освоения практики обучающийся должен

3.1	**Знать:**
3.1.1	способы применения математического аппарата в профессиональной деятельности; основные направления информационной безопасности; классификацию защищаемой информации; классификацию угроз защищаемой информации; возможные методы и пути реализации угроз защищаемой информации.
3.2	**Уметь:**
3.2.1	находить способы использования основных естественнонаучных законов; использовать программные и аппаратные средства персонального компьютера; выбирать показатели качества и критерии оценки систем и средств защиты информации; пользоваться современной научно-технической информацией по вопросам безопасности; выявлять угрозы информационной безопасности объекта.
3.3	**Владеть:**
3.3.1	навыками выявления сущности проблем, возникающих в профессиональной деятельности; навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности; навыками работы с нормативными правовыми актами; методами формирования требований по защите информации; методами и средствами анализа информационной безопасности объекта.

4. СОДЕРЖАНИЕ ПРАКТИКИ					
Код занятия	**Наименование разделов и тем /вид занятия/**	**Семестр / Курс**	**Часов (академических)**	**Компетенции**	**Литература**
	Раздел 1. Общие сведения об организации - базе практики				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Ср/	6	2	ОК-5 ОК-7 ОК-8 ПК-14	Л1.5 Л2.2 Л3.1 Э5

1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	6	2	ПК-14	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 2. Изучение нормативной документации и реализованной инфраструктуры информационной безопасности на предприятии				
2.1	Техническая и сетевая инфраструктура предприятия. Изучение схем информационных потоков в организации. Анализ соответствия защиты информационной безопасности организации в соответствии с нормативными актами предприятия. Анализ современных требований по организации защиты информации на предприятии и сопоставление уровня защиты информации с современными требованиями нормативных и правовых актов Российской Федерации. Конфигурация оборудования в соответствии с нормативными актами предприятия /Ср/	6	60	ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-7 ПК-14	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
2.2	Изучение, систематизация, анализ и сбор материала для формирования отчета по практике; Формирование отчета о прохождении практики, включая выполнение индивидуального задания; Ведение студенческой аттестационной книжки, включая получение отзыва руководителя предприятия /Ср/	6	36	ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-7 ПК-14	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Промежуточная аттестация				
3.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	6	8	ОК-7 ОК-8 ОПК-1 ОПК-2 ОПК-3 ОПК-4 ОПК-5 ОПК-7	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л3.1 Э1 Э2 Э3 Э4 Э5

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	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	

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.2	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальности "Информационная безопасность"	Москва: Академия, 2009	
Л1.3	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	
Л1.4	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	http://e.lanbook.com/books/element.php?pl1_id=59241
Л1.5	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.6	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644
6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Рос. НИИ и проектно-конструкторский ин-т информатизации, автоматизации и связи, Отделение информации (ЦНИИТЭИ)	Указатель документов, действующих в ОАО "РЖД": указатель	Москва, 2004	
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688
Л2.3	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=927768
6.1.3. Методические материалы				
	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"				
Э1	КонсультантПлюс - надежная правовая поддержка (http://www.consultant.ru)			
Э2	Федеральная служба по техническому и экспортному контролю (https://fstec.ru/)			
Э3	Федеральная служба безопасности Российской Федерации (http://www.fsb.ru/)			
Э4	Среда электронного обучения BlackBoard Learn (https://bb.usurt.ru/)			
Э5	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)			
6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)				

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	Операционная система Astra Linux
6.3.1.4	ESET NOD32 Antivirus
6.3.1.5	Платформа управления базами данных: SQL Server
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Abbyy FineReader
6.3.1.8	Adobe Acrobat
6.3.1.9	Система электронной поддержки обучения Blackboard Learn
6.3.1.10	Secret Net Studio
6.3.1.11	Система защиты информации от несанкционированного доступа: Dallas Lock
6.3.1.12	Linux Debian
6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант Плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ	
Назначение	Оснащение
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
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 киптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппартные средства аутетификации 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
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
База практики (Материальная техническая база профильной организации)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети Интернет Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях для конкретных видов работ
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	Специализированная мебель

консультаций	
Учебная аудитория для проведения текущего контроля и промежуточной аттестации (Компьютерные классы)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.04(П) Производственная практика (проектно-технологическая практика)

программа практики

Закреплена за кафедрой Информационные технологии и защита информации

Учебный план 10.03.01 ИБ 3+ 2018.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Специализация

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **6 ЗЕТ**

Способ проведения Стационарный, выездной

Форма проведения Дискретная

Продолжительность 4 недель

Часов по учебному плану	216	Часов контактной работы всего, в том числе:	4
в том числе:		руководство производственной практикой	4
аудиторные занятия	0		
самостоятельная работа	216		

Промежуточная аттестация и формы контроля:
зачет с оценкой 7

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**7 (4.1)**		Итого	
Недель	18			
Вид занятий	УП	РПД	УП	РПД
Сам. работа	216	216	216	216
Итого	216	216	216	216

Программу составил(и):
старший преподаватель, Гузенкова Е.А. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В.В. Башуров

Руководитель ОП ВО _____ / Т.Ю. Гуденкова

Управление информатизации _____ / А.А. Толочинцев

Издательско-библиотечный комплекс _____ / А.А. Колтышев

Учебно-методический отдел _____ / Е.Н. Морозова

Отдел производственного обучения и связи с производством _____ / А.Н. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Кикоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Производственная практика (проектно-технологическая практика)

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: получения профессиональных умений и опыта профессиональной деятельности
1.2	Задачи практики: приобретение практических навыков по организации защиты информации на объектах практики. Ознакомление с используемыми на объектах практики программными и техническими средствами защиты информации. Ознакомление с вопросами метрологии, стандартизации и оценки качества, а также с вопросами организации, планирования и управления предприятием

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах и практиках:
Криптографические методы защиты информации
Техническая защита информации
Безопасность информационных процессов
Безопасность сетей ЭВМ
Документоведение
Конфиденциальный документооборот
Учебная практика (ознакомительная практика)
Учебная практика (практика по получению первичных профессиональных умений и навыков)
Учебная практика (технологическая практика)
Правовые и экономические аспекты профессиональной деятельности
Организационное и правовое обеспечение информационной безопасности
В результате изучения предыдущих дисциплин и(или) разделов дисциплин, а также практик у студентов сформированы:
Знания: системы управления базами данных; назначение и состав операционных систем, основные характеристики, алгоритмы диспетчеризации процессов, операционные системы персональных ЭВМ, основные понятия и методы математической логики и теории алгоритмов диспетчеризации, способы проверки операционных систем на безопасность использования различных программных и аппаратных средств.
Умения: выбирать необходимые инструментальные средства для разработки программ в различных операционных системах и средах; составлять, тестировать, отлаживать программы на языках высокого уровня, включая объектно-ориентированные. самостоятельно работать с учебной, справочной и учебно-методической литературой; определять предельные параметры информационных потоков, обрабатываемых вычислительным комплексом; моделировать операции по распределению ресурсов между процессами, формулировать и настраивать политику безопасности распространенных операционных построенных на их основе вычислительных сетей, систем, а также локальных вычислительных сетей, построенных на их основе, проверять операционные системы на безопасность использования различных программных и аппаратных средств.
Владения: методами анализа и формализации информационных процессов объекта и связей между ними.
навыками работы с учебной и учебно-методической литературой; методами и средствами выявления угроз безопасности операционных системам, методами количественного анализа процессов обработки, поиска и передачи информации.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Защита и обработка конфиденциальных документов
Управление информационной безопасностью на объектах транспортной инфраструктуры
Комплексные системы защиты информации на транспорте
Программно-аппаратные средства защиты информации
Производственная практика (эксплуатационная практика)
Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	
Знать:	
Уровень 1	социальные различия членов коллектива
Уровень 2	общие представления о кооперации с коллегами, работе в коллективе
Уровень 3	культурную и профессиональную речь при общении в работе с коллективом
Уметь:	
Уровень 1	толерантно воспринимать социальные и культурные различия, при работе в группе
Уровень 2	распределять ресурсы коллектива для увеличения производительности работ
Уровень 3	использовать социальные различия в работе коллектива, для увеличения производительности работы
Владеть:	
Уровень 1	анализом определения совместимости членов коллектива по работе с системой информационной безопасности
Уровень 2	методами работы с коллективом
Уровень 3	культурной и профессиональной речью при общении в работе с коллективом

ОК-8: способностью к самоорганизации и самообразованию	
Знать:	
Уровень 1	способы самоорганизации
Уровень 2	методы самообразования
Уровень 3	эффективную методику организации и распределения рабочего времени для сбора и обработки информации
Уметь:	
Уровень 1	организовать самостоятельную работу с источниками информации
Уровень 2	организовывать самостоятельную работу с иностранными источниками информации
Уровень 3	проводить самостоятельно анализ собранной информации и делать выводы, по полученным результатам
Владеть:	
Уровень 1	средствами самоорганизации
Уровень 2	методами самообразования
Уровень 3	эффективной методикой организации и распределения рабочего времени для сбора и обработки информации

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	
Знать:	
Уровень 1	мероприятия по охране труда и технике безопасности
Уровень 2	основные средства защиты персонала предприятия при работе с оборудованием
Уровень 3	основные методы оказания первой помощи в чрезвычайных ситуациях
Уметь:	
Уровень 1	оказывать первую помощь
Уровень 2	использовать персональные средства защиты
Уровень 3	организовывать мероприятия по охране труда и технике безопасности
Владеть:	
Уровень 1	методикой оказания первой медицинской помощи
Уровень 2	средствами защиты персонала предприятия и населения в условиях чрезвычайных ситуаций
Уровень 3	методами организации мероприятий по охране труда и технике безопасности

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	техническую документацию на средства технической защиты
Уровень 2	техническую документацию на программно-аппаратные средства (в том числе криптографические)
Уровень 3	знать технику безопасности обращения с приборами
Уметь:	
Уровень 1	устанавливать технические средства защиты информации
Уровень 2	устанавливать программно-аппаратные
Уровень 3	грамотно эксплуатировать средства в соответствии с их технико-эксплуатационной документацией
Владеть:	
Уровень 1	методикой выполнения работ по установке и настройке программных средств защиты информации
Уровень 2	методикой выполнения работ по установке и настройке аппаратных средств защиты информации
Уровень 3	методикой выполнения работ по установке и настройке криптографических средств защиты информации

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Знать:	
Уровень 1	способы применения программных средств системного назначения для решения профессиональных задач
Уровень 2	способы применения программных средств прикладного назначения для решения профессиональных задач
Уровень 3	способы применения программных средств специального назначения для решения профессиональных задач
Уметь:	
Уровень 1	использовать программные и аппаратные средства персонального компьютера
Уровень 2	выбирать показатели качества систем и средств защиты информации
Уровень 3	выбирать критерии оценки систем и средств защиты информации

Владеть:	
Уровень 1	способами применения программных средств системного назначения для решения профессиональных задач
Уровень 2	способами применения программных средств прикладного назначения для решения профессиональных задач
Уровень 3	способами применения программных средств специального назначения для решения профессиональных задач

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	средства администрирования подсистемы безопасности объектов защиты встроенных в операционные системы
Уровень 2	средства администрирования подсистемы безопасности объектов защиты от сторонних производителей
Уровень 3	средства администрирования подсистемы безопасности объектов защиты с помощью средств, сертифицированных органами регуляторами
Уметь:	
Уровень 1	производить настройку подсистем защиты объекта в соответствии с распорядительными документами организации
Уровень 2	производить анализ существующей конфигурации оборудования для обеспечения соответствия с распорядительными документами организации
Уровень 3	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Владеть:	
Уровень 1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений
Уровень 2	навыками выявления и уничтожения компьютерных вирусов
Уровень 3	навыками анализа информационных потоков в организации и составлением регламента для обеспечения защиты критически важной информации

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знать:	
Уровень 1	методику реализации политики безопасности на объекте практики
Уровень 2	комплексный подход к обеспечению информационной безопасности объектов защиты
Уровень 3	способы формирования политики безопасности
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
Уровень 2	реализовывать повилику информационной безопасности в соответствии с современными требованиями к безопасности объекта защиты
Уровень 3	применять комплексный подход к обеспечению информационной безопасности объекта защиты
Владеть:	
Уровень 1	методикой реализации политики безопасности на объекте практики
Уровень 2	комплексным подходом к обеспечению информационной безопасности объектов защиты
Уровень 3	способом формирования политики безопасности

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем; проводить экспертизу технико-экономического обоснования проектных решений
Уровень 2	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Уровень 3	проводить технико-экономическое обоснование соответствующих проектных решений
Владеть:	
Уровень 1	способами формирования политики безопасности операционных систем
Уровень 2	методикой проведения анализа исходных данных для проектирования подсистем и средств обеспечения

	информационной безопасности
Уровень 3	средствами технико-экономического обоснования проектных решений по обеспечению информационной безопасности

ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	оформлять техническую документацию с учетом действующих нормативны и методических документов
Уровень 2	оформлять рабочую документацию с учетом действующих нормативны и методических документов
Уровень 3	оформлять результаты испытаний объекта защиты
Владеть:	
Уровень 1	методологией оформления технической документации с учетом действующих нормативных и методических документов
Уровень 2	методологией оформления документации с учетом действующих нормативных и методических документов
Уровень 3	методологией оформления результатов испытаний объекта защиты

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	провести анализ информации из различных официальных документов и научной литературы
Уровень 2	грамотно применять правовые документы для организации информационной безопасности на предприятии
Уровень 3	составлять требования по безопасности для обеспечения защиты информации предприятия
Владеть:	
Уровень 1	способами проведения анализа информации
Уровень 2	способами применения правовых документов для организации информационной безопасности на предприятии
Уровень 3	методикой составления требований по безопасности для обеспечения защиты информации на предприятии

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	
Знать:	
Уровень 1	методику проведения экспериментов
Уровень 2	методику обработки результатов экспериментов
Уровень 3	методику оценки погрешности и достоверности результатов
Уметь:	
Уровень 1	проводить эксперименты по заданной методике
Уровень 2	производить обработку результатов экспериментов
Уровень 3	проводить оценку погрешности и достоверности результатов
Владеть:	
Уровень 1	методикой проведения экспериментов
Уровень 2	методикой обработки результатов экспериментов
Уровень 3	методикой оценки погрешности и достоверности результатов экспериментов

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

Уметь:	
Уровень 1	принимать участие в проведении экспериментальных исследований системы защиты информации
Уровень 2	составлять положение о наличии уязвимостей в системе безопасности на основании проведенных экспериментальных исследований
Уровень 3	производить конфигурацию средств защиты информации на основе выявленных уязвимостей
Владеть:	
Уровень 1	навыками коллективного участия в проведении эксперимента
Уровень 2	навыками составление обследования объекта защиты информации на основании эксперимента
Уровень 3	навыками исправления выявленных уязвимостей объекта 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	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
Уровень 2	учувствовать в процессе их реализации мер по обеспечению информационной безопасности
Уровень 3	управлять деятельностью служб защиты информации на предприятии
Владеть:	
Уровень 1	способами организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности
Уровень 2	методикой организации мер по обеспечению информационной безопасности
Уровень 3	способами управления деятельности служб защиты информации на предприятии

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	
Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

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.

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	основные принципы построения комплексных систем защиты информации
Уровень 2	основные угрозы безопасности информации и модели нарушителя в информационных системах предприятий в различных сферах деятельности
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 деятельности
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

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	методы аттестации уровня защищенности информационных систем
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

ПСК-3: способностью участвовать в разработке подсистемы управления информационной безопасностью	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	контролировать эффективность принятых мер по обеспечению информационной безопасности
Уровень 2	конфигурировать подсистему управления информационной безопасности в соответствии с принципами формирования политики информационной безопасности в информационных системах
Уровень 3	проводить экспертизу состояния защищенных информационных систем
Владеть:	
Уровень 1	методикой контроля эффективности принятых мер по обеспечению информационной безопасности
Уровень 2	методами конфигурирования подсистемы управления информационной безопасности
Уровень 3	способами проведения экспертизы состояния защищенности информационных систем

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 практики обучающийся должен

3.1	**Знать:**
3.1.1	методики разработки комплекса мер для обеспечения информационной безопасности информационных систем.
3.2	**Уметь:**
3.2.1	осуществлять противодействие нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
3.3	**Владеть:**
3.3.1	во владении методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература
	Раздел 1. Общие сведения об организации - базе практики				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Ср/	7	2	ОК-6 ОК-8 ОПК-6	Л1.5 Л2.2 Л2.3 Л3.1 Э1 Э4

1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	7	2	ОК-6 ОК-8	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 2. Организация и нормативная документация объекта практики				
2.1	Организационная структура предприятия. Функции отделов и служб /Ср/	7	4	ПК-7 ПК-8 ПК-9 ПК-12	Л1.1 Л2.1 Л3.1 Э1 Э2 Э3 Э5
2.2	Технология работы объекта практики /Ср/	7	4	ПК-7 ПК-8	Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э5
2.3	Нормативные и правовые акты предприятия /Ср/	7	40	ПК-9 ПК-13 ПК-14	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
2.4	Информационные средства и компьютерные программы, применяемые на предприятии /Ср/	7	20	ПК-15 ПСК-2 ПСК-3	Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э5
	Раздел 3. Обследование сетевой инфраструктуры объекта практики				
3.1	Сетевая структура объекта практики /Ср/	7	10	ПК-7 ПК-9	Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3
3.2	Техническое оснащение объекта практики средствами по защите информации /Ср/	7	20	ПК-1 ПК-2 ПК-3 ПК-4 ПК-7 ПК-8 ПК-9 ПК-11 ПК-12	Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3
3.3	Установленные средства обеспечения информационной безопасности на объекте практики /Ср/	7	30	ПК-1 ПК-2 ПК-3	Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3
3.4	Обследование сетевой инфраструктуры и установленных средств по защите информации на соответствие нормативным и правовым актам предприятия /Ср/	7	30	ПК-7 ПК-8 ПК-9 ПК-14 ПК-15 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4
3.5	Аудит обеспечения информационной безопасности в соответствии с требованиями нормативных и правовых актов Российской Федерации /Ср/	7	10	ПК-7 ПК-12 ПК-13 ПСК-1 ПСК-2 ПСК-6	Л1.1 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4
3.6	Выполнение индивидуального задания /Ср/	7	20	ПК-7 ПК-8 ПК-9 ПК-11 ПК-12 ПК-13 ПК-14 ПК-15 ПСК-1 ПСК-2 ПСК-3 ПСК-5 ПСК-6	Л1.3 Л1.4 Л1.6 Л2.1 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 4. Промежуточная аттестация				

4.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	7	24	ОК-8 ПК-4 ПК-7 ПК-9 ПК-13 ПСК-1 ПСК-3 ПСК-5 ПСК-6	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	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	
Л1.2	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальности "Информационная безопасность"	Москва: Академия, 2009	
Л1.3	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	
Л1.4	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	http://e.lanbook.com/books/element.php?pl1_id=59241
Л1.5	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.6	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644

6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Рос. НИИ и проектно-конструкторский ин-т информатизации, автоматизации и связи, Отделение информации (ЦНИИТЭИ)	Указатель документов, действующих в ОАО "РЖД": указатель	Москва, 2004	
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688
Л2.3	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=927768

6.1.3. Методические материалы

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"

Э1	КонсультантПлюс - надежная правовая поддержка (http://www.consultant.ru)
Э2	Федеральная служба по техническому и экспортному контролю (https://fstec.ru/)
Э3	Федеральная служба безопасности Российской Федерации (http://www.fsb.ru/)
Э4	Среда электронного обучения BlackBoard Learn (https://bb.usurt.ru/)
Э5	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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	Операционная система Astra Linux
6.3.1.4	ESET NOD32 Antivirus
6.3.1.5	Платформа управления базами данных: SQL Server
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Abbyy FineReader
6.3.1.8	Adobe Acrobat
6.3.1.9	Система электронной поддержки обучения Blackboard Learn
6.3.1.10	Secret Net Studio
6.3.1.11	Система защиты информации от несанкционированного доступа: Dallas Lock
6.3.1.12	Linux Debian

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант Плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Назначение	Оснащение
Читальный зал Информационно-	Специализированная мебель Компьютерная техника с возможностью подключения к сети "Интернет" и обеспечением

библиотечного центра ИБК УрГУПС - Аудитория для самостоятельной работы	доступа в электронную информационно-образовательную среду Университета
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
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
Учебная аудитория для проведения текущего контроля и промежуточной аттестации (Компьютерные классы)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.05(П) Производственная практика (эксплуатационная практика)

программа практики

Закреплена за кафедрой	Информационные технологии и защита информации		
Учебный план	10.03.01 ИБ 3+ 2018.plx Направление подготовки 10.03.01 Информационная безопасность Направленность (профиль) "Организация и технология защиты информации (на транспорте)"		
Специализация			
Квалификация	**Бакалавр**		
Форма обучения	**очная**		
Объем дисциплины (модуля)	**3 ЗЕТ**		
Способ проведения	Стационарный, выездной		
Форма проведения	Дискретная		
Продолжительность	2 недель		
Часов по учебному плану	108	Часов контактной работы всего, в том числе:	2
в том числе:		руководство производственной практикой	2
аудиторные занятия	0		
самостоятельная работа	108		
Промежуточная аттестация и формы контроля: зачет с оценкой 8			

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Вид занятий	УП	РПД	УП	РПД
Сам. работа	108	108	108	108
Итого	108	108	108	108

Программу составил(и):
старший преподаватель, Гузенкова Е.А. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В. В. Бакуров

Руководитель ОП ВО _____ / Т. Ю. Зорникова

Управление информатизации _____ / А. А. Толочиенуев

Издательско-библиотечный комплекс _____ / А. А. Каптанив

Учебно-методический отдел _____ / Е. Н. Морозова

Отдел производственного обучения и связи с производством _____ / А. М. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Кикоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Производственная практика (эксплуатационная практика)

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: получение профессиональных умений и опыта в профессиональной деятельности
1.2	Задачи: приобретение практических навыков по конфигурированию и монтажу оборудования защиты информации, программно-аппаратных, программах и технических средств применяемого на объекте практики. Изучение нормативной и правовой документации по информационной безопасности на объекте практики. Формирование комплекса мер по защите информации, конфигурирование оборудования и программного обеспечения в соответствии с ним.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах и практиках:
Техническая защита информации
Безопасность информационных процессов
Безопасность сетей ЭВМ
Комплексные системы защиты информации на транспорте
Защита информационных процессов на транспорте
Управление информационной безопасностью на объектах транспортной инфраструктуры
Защита и обработка конфиденциальных документов
Производственная практика (проектно-технологическая практика)
Организационное и правовое обеспечение информационной безопасности
Программно-аппаратные средства защиты информации
В результате изучения предыдущих дисциплин и(или) разделов дисциплин, а также практики у студентов сформированы:
Знания: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации. методы формирования политики безопасности объектов защиты; российские и международные стандарты в области информационной безопасности; аппаратные средства вычислительной техники; принципы построения информационных систем; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Умения: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.
Владения: навыками анализа активов организации, их угроз информационной безопасности и уязвимостей в рамках области деятельности.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Преддипломная практика

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОК-6: способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	
Знать:	
Уровень 1	социальные различия членов коллектива
Уровень 2	общие представления о кооперации с коллегами, работе в коллективе
Уровень 3	культурную и профессиональную речь при общении в работе с коллективом
Уметь:	
Уровень 1	толерантно воспринимать социальные и культурные различия, при работе в группе
Уровень 2	распределять ресурсы коллектива для увеличения производительности работ
Уровень 3	использовать социальные различия в работе коллектива, для увеличения производительности работы
Владеть:	
Уровень 1	анализом определения совместимости членов коллектива по работе с системой информационной безопасности
Уровень 2	методами работы с коллективом
Уровень 3	культурной и профессиональной речью при общении в работе с коллективом

ОК-8: способностью к самоорганизации и самообразованию	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-

Уметь:	
Уровень 1	организовать самостоятельную работу с источниками информации
Уровень 2	организовывать самостоятельную работу с иностранными источниками информации
Уровень 3	проводить самостоятельно анализ собранной информации и делать выводы, по полученным результатам
Владеть:	
Уровень 1	средствами самоорганизации
Уровень 2	методами самообразования
Уровень 3	эффективной методикой организации и распределения рабочего времени для сбора и обработки

ОПК-6: способностью применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций, организовать мероприятия по охране труда и технике безопасности	
Знать:	
Уровень 1	мероприятия по охране труда и технике безопасности
Уровень 2	основные средства защиты персонала предприятия при работе с оборудованием
Уровень 3	основные методы оказания первой помощи в чрезвычайных ситуациях
Уметь:	
Уровень 1	применять приемы оказания первой помощи, методы и средства защиты персонала предприятия и населения в условиях чрезвычайных ситуаций
Уровень 2	организовать мероприятия по охране труда и технике безопасности
Уровень 3	-
Владеть:	
Уровень 1	методикой оказания первой медицинской помощи
Уровень 2	средствами защиты персонала предприятия и населения в условиях чрезвычайных ситуаций
Уровень 3	методами организации мероприятий по охране труда и технике безопасности

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	техническую документацию на средства технической защиты
Уровень 2	техническую документацию на программно-аппаратные средства (в том числе криптографические)
Уровень 3	знать технику безопасности обращения с приборами
Уметь:	
Уровень 1	устанавливать технические средства защиты информации
Уровень 2	устанавливать программно-аппаратные
Уровень 3	грамотно эксплуатировать средства в соответствии с их технико-эксплуатационной документацией
Владеть:	
Уровень 1	методикой выполнения работ по установке и настройке программных средств защиты информации
Уровень 2	методикой выполнения работ по установке и настройке аппаратных средств защиты информации
Уровень 3	методикой выполнения работ по установке и настройке криптографических средств защиты информации

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	использовать программные и аппаратные средства персонального компьютера;
Уровень 2	выбирать показатели качества систем и средств защиты информации
Уровень 3	выбирать критерии оценки систем и средств защиты информации
Владеть:	
Уровень 1	способами применения программных средств системного назначения для решения профессиональных задач
Уровень 2	способами применения программных средств прикладного назначения для решения профессиональных задач
Уровень 3	способами применения программных средств специального назначения для решения профессиональных задач

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	производить настройку подсистем защиты объекта в соответствии с распорядительными документами организации
Уровень 2	производить анализ существующей конфигурации оборудования для обеспечения соответствия с распорядительными документами организации
Уровень 3	осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты
Владеть:	
Уровень 1	методикой анализа сетевого трафика, результатов работы средств обнаружения вторжений
Уровень 2	навыками выявления и уничтожения компьютерных вирусов
Уровень 3	навыками анализа информационных потоков в организации и составлением регламента для обеспечения защиты критически важной информации

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знать:	
Уровень 1	методику реализации политики безопасности на объекте практики
Уровень 2	комплексный подход к обеспечению информационной безопасности объектов защиты
Уровень 3	способы формирования политики безопасности
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
Уровень 2	реализовывать политику информационной безопасности в соответствии с современными требованиями к безопасности объекта защиты
Уровень 3	применять комплексный подход к обеспечению информационной безопасности объекта защиты
Владеть:	
Уровень 1	методикой реализации политики безопасности на объекте практики
Уровень 2	комплексным подходом к обеспечению информационной безопасности объектов защиты
Уровень 3	способом формирования политики безопасности

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Знать:	
Уровень 1	основы организационного и правового обеспечения информационной безопасности; нормативные методические документы ФСБ России и ФСТЭК России в области защиты объекта информатизации
Уровень 2	нормативные методические документы ФСБ России и ФСТЭК России в области защиты объекта информатизации
Уровень 3	нормативные документы по безопасности, разработанные в организации
Уметь:	
Уровень 1	осуществлять правовую оценку объекта информатизации
Уровень 2	применять нормативные правовые акты и нормативные методические документы в области информационной безопасности при аттестации объекта информатизации
Уровень 3	проводить аттестацию объекта информатизации по требованиям безопасности информации
Владеть:	
Уровень 1	методами осуществления правовой оценки объекта
Уровень 2	способами применения правовых актов и нормативных методических документов в области информационной безопасности
Уровень 3	способами проведения анализа информационной безопасности объекта

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	методику организации контрольных проверок работоспособности программно-аппаратных средств защиты информации
Уровень 2	методику проведения контрольных проверок работоспособности и эффективности программно-аппаратных

	средств защиты информации
Уровень 3	нормативные документы, посредством которых организуется проведение контрольных проверок применяемых средств защиты информации
Уметь:	
Уровень 1	использовать методику контрольных проверок работоспособности и эффективности программных средств защиты информации
Уровень 2	использовать методику контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	использовать методику контрольных проверок работоспособности и эффективности технических средств защиты информации
Владеть:	
Уровень 1	методами анализа работоспособности и эффективности программных средств защиты информации
Уровень 2	методами анализа работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	методами анализа работоспособности и эффективности технических средств защиты информации

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
Знать:	
Уровень 1	средства для проведения анализа исходных данных для проектирования подсистем и средств защиты
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем; проводить экспертизу технико-экономического обоснования проектных решений
Уровень 2	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Уровень 3	проводить технико-экономическое обоснование соответствующих проектных решений
Владеть:	
Уровень 1	способами формирования политики безопасности операционных систем
Уровень 2	методикой проведения анализа исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Уровень 3	средствами технико-экономического обоснования проектных решений по обеспечению информационной безопасности

ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	
Знать:	
Уровень 1	действующие нормативные и методические документы по оформлению технической документации
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	оформлять техническую документацию с учетом действующих нормативны и методических документов
Уровень 2	оформлять рабочую документацию с учетом действующих нормативны и методических документов
Уровень 3	оформлять результаты испытаний объекта защиты
Владеть:	
Уровень 1	методологией оформления технической документации с учетом действующих нормативных и методических документов
Уровень 2	методологией оформления документации с учетом действующих нормативных и методических документов
Уровень 3	методологией оформления результатов испытаний объекта защиты

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	

Уровень 1	провести анализ информации из различных официальных документов и научной литературы
Уровень 2	грамотно применять правовые документы для организации информационной безопасности на предприятии
Уровень 3	составлять требования по безопасности для обеспечения защиты информации предприятия
Владеть:	
Уровень 1	способами проведения анализа информации
Уровень 2	способами применения правовых документов для организации информационной безопасности на предприятии
Уровень 3	методикой составления требований по безопасности для обеспечения защиты информации на предприятии

ПК-13: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
Уровень 2	учувствовать в процессе их реализации мер по обеспечению информационной безопасности
Уровень 3	управлять деятельностью служб защиты информации на предприятии
Владеть:	
Уровень 1	способами организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности
Уровень 2	методикой организации мер по обеспечению информационной безопасности
Уровень 3	способами управления деятельности служб защиты информации на предприятии

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	
Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

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	основные принципы построения комплексных систем защиты информации
Уровень 2	основные угрозы безопасности информации и модели нарушителя в информационных системах предприятий в различных сферах деятельности
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 деятельности
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

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	методы аттестации уровня защищенности информационных систем
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

ПСК-3: способностью участвовать в разработке подсистемы управления информационной безопасностью	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	контролировать эффективность принятых мер по обеспечению информационной безопасности
Уровень 2	конфигурировать подсистему управления информационной безопасности в соотвествии с принципами формирования политики информационной безопасности в информационных системах
Уровень 3	проводить экспертизу состояния защищенных информационных систем
Владеть:	
Уровень 1	методикой контроля эффективности принятых мер по обеспечению информационной безопасности
Уровень 2	методами конфигурирования подсистемы управления информационной безопасности
Уровень 3	способами проведения экспертизы состояния защищенности информационных систем

В результате освоения практики 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 противодействие нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
3.3	**Владеть:**
3.3.1	во владении методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература
	Раздел 1. Общие сведения об организации - базе практики				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Ср/	8	2	ОК-6 ОК-8 ОПК-6	Л1.5 Л2.2 Л2.3 Л3.1 Э4

1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	8	2	ОК-6 ОК-8	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
1.3	Технология работы объекта практики /Ср/	8	5	ОК-6	Л1.1 Л2.1 Л3.1 Э1 Э2 Э3
1.4	Нормативные и правовые акты предприятия /Ср/	8	10	ПК-5 ПК-9	Л1.1 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
1.5	Информационные средства и компьютерные программы, применяемые на предприятии /Ср/	8	8	ПК-1 ПК-2	Л1.3 Л2.1 Л3.1 Э1 Э2 Э3
	Раздел 2. Эксплуатация средств защиты информации				
2.1	Обзор средства защиты информации установленные на объекте практики /Ср/	8	4	ПК-2	Л1.3 Л1.4 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
2.2	Изучение технической документации на устройства защиты информации /Ср/	8	8	ПК-9	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
2.3	Работа с нормативными и правовыми документами /Ср/	8	10	ПК-8 ПК-9	Л1.1 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
2.4	Организация работы коллектива по организации информационной безопасности на предприятии /Ср/	8	2	ПК-14	Л1.1 Л2.1 Л3.1 Э1 Э2 Э3
2.5	Эксплуатация программных, программно-аппаратных и технических средств прикладного и системного назначения /Ср/	8	5	ПК-1 ПК-2	Л1.2 Л1.3 Л1.4 Л2.1 Л3.1 Э1 Э2 Э3
2.6	Установка, конфигурирование и обслуживание средств защиты информации /Ср/	8	8	ПК-1 ПК-2 ПК-3 ПК-6	Л1.3 Л2.1 Л3.1 Э1 Э2 Э3
2.7	Администрирование подсистемы информационной безопасности на объекте защиты /Ср/	8	8	ПК-1 ПК-2 ПК-3 ПК-6	Л1.2 Л1.3 Л1.4 Л2.1 Л3.1 Э1 Э2 Э3
2.8	Сопровождение и аттестация объекта информатизации на соответствии требованиям по защите информации /Ср/	8	4	ПК-5 ПК-13 ПСК-1 ПСК-2 ПСК-3	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3
2.9	Эксплуатация подсистем управления информационной безопасности /Ср/	8	5	ПК-5 ПСК-2 ПСК-3	Л1.1 Л1.2 Л1.3 Л2.1 Л3.1 Э1 Э2 Э3
2.10	Мониторинг работоспособности и анализ эффективности реализованных мер защиты информации на объекте практики /Ср/	8	4	ПК-2 ПК-5 ПК-6 ПСК-2	Л1.2 Л1.3 Л1.4 Л2.1 Л3.1 Э1 Э2 Э3 Э5

2.11	Выполнение индивидуального задания /Ср/	8	10	ОК-8 ПК-2 ПК-3 ПК-4 ПК-5 ПК-6 ПК-7 ПК-8 ПК-9 ПК-13 ПК-14 ПСК-1 ПСК-2 ПСК-3	Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Промежуточная аттестация				
3.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	8	13	ПК-6 ПК-7 ПК-8 ПК-9 ПК-13	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики.

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	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	
Л1.2	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальности "Информационная безопасность"	Москва: Академия, 2009	
Л1.3	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	
Л1.4	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	http://e.lanbook.com/books/element.php?pl1_id=59241

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.5	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.6	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644

6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Рос. НИИ и проектно-конструкторский ин-т информатизации, автоматизации и связи, Отделение информации (ЦНИИТЭИ)	Указатель документов, действующих в ОАО "РЖД": указатель	Москва, 2004	
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688
Л2.3	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=927768

6.1.3. Методические материалы

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"

Э1	КонсультантПлюс - надежная правовая поддержка (http://www.consultant.ru)
Э2	Федеральная служба по техническому и экспортному контролю (https://fstec.ru/)
Э3	Федеральная служба безопасности Российской Федерации (http://www.fsb.ru/)
Э4	Среда электронного обучения BlackBoard Learn (https://bb.usurt.ru/)
Э5	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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	Операционная система Astra Linux
6.3.1.4	ESET NOD32 Antivirus
6.3.1.5	Платформа управления базами данных: SQL Server
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Abbyy FineReader
6.3.1.8	Adobe Acrobat
6.3.1.9	Система электронной поддержки обучения Blackboard Learn
6.3.1.10	Secret Net Studio
6.3.1.11	Система защиты информации от несанкционированного доступа: Dallas Lock

6.3.1.12	Linux Debian

6.3.2 Перечень информационных справочных систем и профессиональных баз данных	
6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Назначение	Оснащение
Учебная аудитория для проведения текущего контроля и промежуточной аттестации (Компьютерные классы)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, 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
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

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
"Уральский государственный университет путей сообщения"

(ФГБОУ ВО УрГУПС)

Б2.В.06(Пд) Преддипломная практика

программа практики

Закреплена за кафедрой Информационные технологии и защита информации

Учебный план 10.03.01 ИБ 3+ 2018.plx
Направление подготовки 10.03.01 Информационная безопасность
Направленность (профиль) "Организация и технология защиты информации (на транспорте)"

Специализация

Квалификация **Бакалавр**

Форма обучения **очная**

Объем дисциплины (модуля) **9 ЗЕТ**

Способ проведения Стационарный, выездной

Форма проведения Дискретная

Продолжительность 6 недель

Часов по учебному плану	324	Часов контактной работы всего, в том числе:	3
в том числе:		руководство производственной, преддипломной практикой	3
аудиторные занятия	0		
самостоятельная работа	324		

Промежуточная аттестация и формы контроля:
зачет с оценкой 8

Распределение часов практики по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Вид занятий	УП	РПД	УП	РПД
Сам. работа	324	324	324	324
Итого	324	324	324	324

Программу составил(и):
старший преподаватель, Гузенкова Е.А. _____

Согласовано:

Кафедра Информационные технологии и защита информации _____ / В. В. Башуров

Руководитель ОП ВО _____ / Т. Ю. Зиганшина.

Управление информатизации _____ / А. А. Толочиенец

Издательско-библиотечный комплекс _____ / А. А. Колташев

Учебно-методический отдел _____ / Е. Н. Морозова

Отдел производственного обучения и связи с производством _____ / А. Н. Попов

Профильная организация

Начальник отдела контроля и эксплуатации средств защиты информации ЕИВЦ - структурного подразделения ГВЦ – филиала ОАО «РЖД» _____ / *Киоть С. А.*

Директор Екатеринбургского НТЦ ФГУП «НПП «Гамма» _____ / *Худеньких А. С.*

Программа практики
Преддипломная практика

разработана в соответствии с ФГОС: Приказ от 01.12.2016 № 1515

составлена на основании учебного плана:
Направление 10.03.01 Информационная безопасность
Направленность (профиль) № 2 "Организация и технология защиты информации (на транспорте)"

Программа практики одобрена на заседании кафедры
Информационные технологии и защита информации

Протокол от 28 августа 2018 г. № 1

1. ЦЕЛЬ И ЗАДАЧИ ПРАКТИКИ	
1.1	Цель: преддипломная практика проводится для выполнения выпускной квалификационной работы.
1.2	Задачи практики: усовершенствование практических навыков по конфигурации, монтажу оборудования защиты информации, применяемого на объекте практики. Работа с нормативными и правовыми документами, для формирования комплексной защиты информации на объекте практики. Сбор и анализ материала для выполнения квалификационной выпускной работы.

2. МЕСТО ПРАКТИКИ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б2.В

2.1 Требования к предварительной подготовке обучающегося:

Для прохождения практики необходимы знания, умения и навыки, формируемые на предшествующих дисциплинах и практиках:
Программно-аппаратные средства защиты информации
Безопасность информационных процессов
Учебная практика (технологическая)
Производственная практика (проектно-технологическая практика)
Производственная практика (эксплуатационная практика)
Комплексные системы защиты информации на транспорте
Управление информационной безопасностью на объектах транспортной инфраструктуры
Защита информационных процессов на транспорте
Защита и обработка конфиденциальных документов
В результате изучения предыдущих дисциплин и(или) разделов дисциплин, а также практик у студентов сформированы:
Знания: принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
Умения: осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты; анализировать и оценивать угрозы информационной безопасности; применять отечественные и зарубежные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем.
Владения: методами и средствами выявления угроз безопасности автоматизированным системам; методами формирования требований по защите информации; методами анализа и формализации информационных процессов объекта и связей между ними; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

2.2 Дисциплины и практики, для которых освоение данной практики необходимо как предшествующее:

Государственная итоговая аттестация

3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПРИ ПРОХОЖДЕНИИ ПРАКТИКИ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
ОПК-4: способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	
Знать:	
Уровень 1	способы проведения анализа информации и классификация ее в соответствии с требуемым уровнем защищенности.
Уровень 2	информационные технологии для реализации способов защиты информации
Уровень 3	нормативные и методические документы, регламентирующие применение информационных технологий для защиты информации
Уметь:	
Уровень 1	использовать программные и аппаратные средства персонального компьютера
Уровень 2	выбирать показатели качества и критерии оценки систем и средств защиты информации
Уровень 3	пользоваться современной научно-технической информацией по вопросам безопасности
Владеть:	
Уровень 1	навыками поиска нормативной правовой информации, необходимой для профессиональной деятельности
Уровень 2	навыками работы с нормативными правовыми актами
Уровень 3	методами формирования требований по защите информации

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	техническую документацию на средства технической защиты
Уровень 2	техническую документацию на программно-аппаратные средства (в том числе криптографические)
Уровень 3	знать технику безопасности обращения с приборами
Уметь:	

Уровень 1	устанавливать технические средства защиты информации
Уровень 2	устанавливать программно-аппаратные
Уровень 3	грамотно эксплуатировать средства в соответствии с их технико-эксплуатационной документацией
Владеть:	
Уровень 1	методикой конфигурации средств защиты в соответствии с требованиями документов по обеспечению информационной безопасности на предприятии
Уровень 2	методикой конфигурации программного обеспечения по защите информации в соответствии с требованиями документов по обеспечению информационной безопасности на предприятии
Уровень 3	правилами эксплуатации средств защиты информации, в соответствии с их технико-эксплуатационной документацией

ПК-2: способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	использовать программные и аппаратные средства персонального компьютера
Уровень 2	выбирать показатели качества систем и средств защиты информации
Уровень 3	выбирать критерии оценки систем и средств защиты информации
Владеть:	
Уровень 1	правилами использования программных и аппаратных средств персонального компьютера
Уровень 2	методикой по выбору показателей качества систем и средств защиты информации
Уровень 3	методикой по осуществлению выбора критериев оценки систем и средств защиты информации

ПК-3: способностью администрировать подсистемы информационной безопасности объекта защиты	
Знать:	
Уровень 1	средства администрирования подсистемы безопасности объектов защиты встроенных в операционные системы
Уровень 2	средства администрирования подсистемы безопасности объектов защиты от сторонних производителей
Уровень 3	средства администрирования подсистемы безопасности объектов защиты с помощью средств, сертифицированных органами регуляторами
Уметь:	
Уровень 1	администрировать подсистемы безопасности объекта защиты
Уровень 2	производить модернизацию подсистем безопасности объекта защиты в соответствии с руководящими документами
Уровень 3	проводить аудит подсистемы защиты на соответствие требованиям нормативных и методических документов
Владеть:	
Уровень 1	методами администрирования подсистем безопасности объекта защиты
Уровень 2	методикой модернизации систем безопасности объекта защиты, созданной органом регулятором
Уровень 3	методикой проведения аудита подсистемы защиты на соответствие нормативным и правовым документам

ПК-4: способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты	
Знать:	
Уровень 1	методику реализации политики безопасности на объекте практики
Уровень 2	комплексный подход к обеспечению информационной безопасности объектов защиты
Уровень 3	способы формирования политики безопасности
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе
Уровень 2	реализовывать повилику информационной безопасности в соответствии с современными требованиями к безопасности объекта защиты
Уровень 3	применять комплексный подход к обеспечению информационной безопасности объекта защиты
Владеть:	
Уровень 1	методикой реализации политики безопасности на объекте практики
Уровень 2	комплексным подходом к обеспечению информационной безопасности объектов защиты

Уровень 3	способом формирования политики безопасности

ПК-5: способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации	
Знать:	
Уровень 1	основы организационного и правового обеспечения информационной безопасности
Уровень 2	нормативные методические документы ФСБ России и ФСТЭК России в области защиты объекта информатизации
Уровень 3	нормативные документы по безопасности, разработанные в организации
Уметь:	
Уровень 1	осуществлять правовую оценку объекта информатизации
Уровень 2	применять нормативные правовые акты и нормативные методические документы в области информационной безопасности
Уровень 3	производить анализ информационной безопасности объекта
Владеть:	
Уровень 1	методами осуществления правовой оценки объекта
Уровень 2	способами применения правовых актов и нормативных методических документов в области информационной безопасности
Уровень 3	способами проведения анализа информационной безопасности объекта

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	методику организации контрольных проверок работоспособности программно-аппаратных средств защиты информации
Уровень 2	методику проведения контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	нормативные документы, посредством которых организуется проведение контрольных проверок применяемых средств защиты информации
Уметь:	
Уровень 1	использовать методику контрольных проверок работоспособности и эффективности программных средств защиты информации
Уровень 2	использовать методику контрольных проверок работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	использовать методику контрольных проверок работоспособности и эффективности технических средств защиты информации
Владеть:	
Уровень 1	методами анализа работоспособности и эффективности программных средств защиты информации
Уровень 2	методами анализа работоспособности и эффективности программно-аппаратных средств защиты информации
Уровень 3	методами анализа работоспособности и эффективности технических средств защиты информации

ПК-7: способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	
Знать:	
Уровень 1	методику проведения анализа исходных данных предприятия для проектирования подсистем и средств обеспечения информационной безопасности
Уровень 2	методику проведения технико-экономического обоснования проектных решений по реализации подсистем и средств обеспечения информационной безопасности
Уровень 3	способы прогнозирования поведения реализованной системы безопасности при изменении факторов, влияющих на защищенность спроектированной системы
Уметь:	
Уровень 1	формулировать и настраивать политику безопасности распространенных операционных систем; проводить экспертизу технико-экономического обоснования проектных решений
Уровень 2	проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности
Уровень 3	проводить технико-экономическое обоснование соответствующих проектных решений
Владеть:	
Уровень 1	методами конфигурирования политики безопасности распределенных операционных систем
Уровень 2	методами анализа исходных данных при проектировании подсистем и средств обеспечения

	информационной безопасности
Уровень 3	методикой проведения технико-экономического обоснования соответствующих проектных решений

ПК-8: способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	
Знать:	
Уровень 1	действующие нормативные и методические документы для оформления рабочей, технической документации
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	оформлять техническую документацию с учетом действующих нормативных и методических документов
Уровень 2	оформлять рабочую документацию с учетом действующих нормативных и методических документов
Уровень 3	оформлять результаты испытаний объекта защиты
Владеть:	
Уровень 1	методикой оформления технической документации с учетом действующих нормативных и методических документов
Уровень 2	методикой оформления рабочей документации с учетом действующих нормативных и методических документов
Уровень 3	методикой оформления результатов испытаний на объекте защиты

ПК-9: способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
Знать:	
Уровень 1	способы осуществления подбора, изучение и обобщение научно-технической литературы
Уровень 2	требуемые нормативные и методические материалы, для организации информационной безопасности на предприятии
Уровень 3	способы составления обзора информационной безопасности на предприятии посредством анализа внутренней документации по защите информации
Уметь:	
Уровень 1	провести анализ информации из различных официальных документов и научной литературы
Уровень 2	грамотно применять правовые документы для организации информационной безопасности на предприятии
Уровень 3	составлять требования по безопасности для обеспечения защиты информации предприятия
Владеть:	
Уровень 1	методами проведения и обобщения результатов анализа информации, полеченной из различных официальных документов и научной литературы
Уровень 2	средствами грамотного применения правовых документов для организации информационной безопасности на предприятии
Уровень 3	методологией составления требований по безопасности для обеспечения защиты информации на предприятии

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

ПК-11: способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов	
Знать:	
Уровень 1	методику проведения экспериментов
Уровень 2	методику обработки результатов экспериментов
Уровень 3	методику оценки погрешности и достоверности результатов
Уметь:	
Уровень 1	проводить эксперименты по заданной методике
Уровень 2	производить обработку результатов экспериментов
Уровень 3	проводить оценку погрешности и достоверности результатов
Владеть:	
Уровень 1	методикой проведения экспериментов
Уровень 2	методикой обработки результатов экспериментов
Уровень 3	методикой оценки погрешности и достоверности результатов экспериментов

ПК-12: способностью принимать участие в проведении экспериментальных исследований системы защиты информации	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	принимать участие в проведении экспериментальных исследований системы защиты информации
Уровень 2	составлять положение о наличии уязвимостей в системе безопасности на основании проведенных экспериментальных исследований
Уровень 3	производить конфигурацию средств защиты информации на основе выявленных уязвимостей
Владеть:	
Уровень 1	навыками коллективного участия в проведении эксперимента
Уровень 2	навыками составление обследования объекта защиты информации на основании эксперимента
Уровень 3	навыками исправления выявленных уязвимостей объекта 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	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности
Уровень 2	учувствовать в процессе их реализации мер по обеспечению информационной безопасности
Уровень 3	управлять деятельностью служб защиты информации на предприятии
Владеть:	
Уровень 1	способами организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности
Уровень 2	методикой организации мер по обеспечению информационной безопасности
Уровень 3	способами управления деятельности служб защиты информации на предприятии

ПК-14: способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	организовать работу в группе по обеспечению информационной безопасности информационной системы
Уровень 2	организовать работу в группе по настройке и тестированию программно-аппаратных и технических средств
Уровень 3	анализировать предложения участников группы по улучшению информационной защиты организации
Владеть:	

Уровень 1	грамотной речью
Уровень 2	профессиональной терминологией по информационной безопасности
Уровень 3	способами распределения ролей участников группы

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.

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	основные принципы построения комплексных систем защиты информации
Уровень 2	основные угрозы безопасности информации и модели нарушителя в информационных системах предприятий в различных сферах деятельности
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 деятельности
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

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	методы аттестации уровня защищенности информационных систем
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

ПСК-3: способностью участвовать в разработке подсистемы управления информационной безопасностью	
Знать:	
Уровень 1	-
Уровень 2	-
Уровень 3	-
Уметь:	
Уровень 1	контролировать эффективность принятых мер по обеспечению информационной безопасности
Уровень 2	конфигурировать подсистему управления информационной безопасности в соответствии с принципами формирования политики информационной безопасности в информационных системах
Уровень 3	проводить экспертизу состояния защищенных информационных систем
Владеть:	
Уровень 1	методикой контроля эффективности принятых мер по обеспечению информационной безопасности
Уровень 2	методами конфигурирования подсистемы управления информационной безопасности
Уровень 3	способами проведения экспертизы состояния защищенности информационных систем

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-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 практики обучающийся должен

3.1	**Знать:**
3.1.1	организационные основы и принципы деятельности службы защиты информации (СЗИ); нормативно-правовые акты и руководящие документы по вопросам работы СЗИ; теоретически и практически изучить методы и технологии управления СЗИ; принципы и методы противодействия несанкционированному информационному воздействию на вычислительные системы и системы передачи информации.
3.2	**Уметь:**
3.2.1	анализировать и оценивать угрозы информационной безопасности объекта; осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты.
3.3	**Владеть:**
3.3.1	владения методами анализа и формализации информационных процессов объекта и связей между ними; методами организации и управления деятельностью служб защиты информации на предприятии; методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.

4. СОДЕРЖАНИЕ ПРАКТИКИ

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов (академических)	Компетенции	Литература
	Раздел 1. Общие сведения об организации - базе практики				
1.1	Инструктаж по технике безопасности, правилам внутреннего распорядка организации и правилам охраны труда /Ср/	8	8	ОПК-4	Л1.5 Л2.2 Л2.3 Л3.1 Э1
1.2	Обсуждение совместного рабочего графика (плана) проведения практики с руководителем практики от производства, порядок его реализации /Ср/	8	10	ОПК-4	Л1.1 Л1.2 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л2.3 Л3.1 Э1
1.3	Технология работы объекта практики /Ср/	8	10	ПК-7	Л1.1 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
1.4	Нормативные и правовые акты предприятия /Ср/	8	40	ПК-9 ПК-10 ПК-15 ПСК-4 ПСК-5	Л1.1 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
1.5	Информационные средства и компьютерные программы, применяемые на предприятии /Ср/	8	40	ПК-1 ПК-2 ПК-15	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5

	Раздел 2. Сбор материала для выполнения выпускной квалификационной работы				
2.1	Анализ исходных данных для проектирования системы информационной безопасности на объекте практики /Ср/	8	20	ПК-7 ПСК-4	Л1.1 Л1.4 Л2.1 Л2.2 Л3.1 Э1 Э2 Э3 Э4 Э5
2.2	Мониторинг работоспособности и анализ эффективности мер, реализуемых на объекте практики /Ср/	8	50	ПК-10 ПК-15 ПСК-4	Л1.1 Л1.3 Л2.1 Л2.2 Л3.1 Э2 Э3
2.3	Работа с технической литературой и нормативными и правовыми документами /Ср/	8	40	ПК-15 ПСК-4	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л3.1 Э1 Э2 Э3 Э4 Э5
2.4	Формирование комплекса мер по обеспечению информационной безопасности на объекте практики /Ср/	8	30	ПК-7 ПК-8 ПК-9 ПК-10 ПК-15 ПСК-4 ПСК-5 ПСК-6	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л2.2 Л3.1 Э1 Э2 Э3 Э4 Э5
2.5	Разработка подсистем управления информационной безопасностью /Ср/	8	20	ПК-1 ПК-2 ПК-8 ПК-15	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
2.6	Оформление рабочей документации с учетом действующих нормативной и технической документации /Ср/	8	10	ПК-8 ПК-9	Л1.1 Л1.6 Л2.1 Л3.1 Э1 Э4
2.7	Формирование требований политики безопасности на объекте практики и ее реализация /Ср/	8	10	ПК-15 ПСК-5 ПСК-6	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э5
2.8	Выполнение индивидуального задания /Ср/	8	21	ПК-8 ПК-15 ПСК-1 ПСК-3 ПСК-4 ПСК-5 ПСК-6	Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5
	Раздел 3. Промежуточная аттестация				
3.1	Подготовка к промежуточной аттестации (защита отчета) /Ср/	8	15	ПК-7 ПК-8 ПК-9 ПК-10 ПСК-4 ПСК-5 ПСК-6	Л1.1 Л1.3 Л1.4 Л1.6 Л2.1 Л3.1 Э1 Э2 Э3 Э4 Э5

5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

5.1 Формы отчетности по практике

Промежуточная аттестация проводится в форме зачета с оценкой, который предполагает защиту обучающимся отчета по практике

5.2 Темы индивидуальных заданий

Конкретное содержание практики определяется обучающимися совместно с руководителями практики от университета, согласуется с руководителем практики от профильной организации и закрепляется в совместном рабочем графике (плане) проведения практики. Индивидуальные задания разрабатываются в зависимости от объекта практики.

5.3 Фонд оценочных средств для проведения промежуточной аттестации по практике

Фонд оценочных средств по практике, состоящий из ФОС для текущего контроля и проведения промежуточной аттестации обучающихся 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 средств для проведения промежуточной аттестации обучающихся по практике, порядок проведения промежуточной аттестации, включая систему оценивания результатов промежуточной аттестации и критерии выставления оценок приведены в приложении 1 к программе практики

6. ПЕРЕЧЕНЬ УЧЕБНОЙ ЛИТЕРАТУРЫ И РЕСУРСОВ СЕТИ "ИНТЕРНЕТ", НЕОБХОДИМЫХ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

6.1 Перечень учебной литературы, нормативных документов, а также методических материалов, необходимых для проведения практики

6.1.1. Учебная литература

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л1.1	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	
Л1.2	Грушо А. А., Применко Э. А., Тимонина Е. Е.	Теоретические основы компьютерной безопасности: учебное пособие для студентов вузов, обучающихся по специальности "Информационная безопасность"	Москва: Академия, 2009	
Л1.3	Платонов В. В.	Программно-аппаратные средства защиты информации: учебник для студентов вузов, обучающихся по направлению подготовки "Информационная безопасность"	Москва: Академия, 2013	
Л1.4	Корниенко А. А.	Информационная безопасность и защита информации на железнодорожном транспорте: в 2-х ч. : рекомендовано Экспертным советом по рецензированию Моск. гос. ун-та путей сообщ. в качестве учебника для студентов, обучающихся по специальности 090302.65 "Информационная безопасность телекоммуникационных систем" ВПО	Москва: Учебно-методический центр по образованию на ж.-д. трансп., 2014	http://e.lanbook.com/books/element.php?pl1_id=59241
Л1.5	Коханов В. Н., Емельянова Л. Д., Некрасов П. А.	Безопасность жизнедеятельности: Учебник	Москва: ООО "Научно-издательский центр ИНФРА-М", 2014	http://znanium.com/go.php?id=395770
Л1.6	Баранова Е. К., Бабаш А. В.	Информационная безопасность и защита информации: Учебное пособие	Москва: Издательский Центр РИО, 2017	http://znanium.com/go.php?id=763644

6.1.2. Нормативные документы, включая нормативные документы ОАО"РЖД"

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л2.1	Рос. НИИ и проектно-конструкторский ин-т информатизации, автоматизации и связи, Отделение информации (ЦНИИТЭИ)	Указатель документов, действующих в ОАО "РЖД": указатель	Москва, 2004	
Л2.2	Без автора	Правила по охране труда при эксплуатации электроустановок	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=924688
Л2.3	Без автора	Конституция Российской Федерации	Москва: ООО "Научно-издательский центр ИНФРА-М", 2018	http://znanium.com/go.php?id=927768

6.1.3. Методические материалы

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка

	Авторы, составители	Заглавие	Издательство, год	Web-ссылка
Л3.1	Гузенкова Е. А., Зырянова Т. Ю.	Организация, проведение и защита практики студентов: методические рекомендации для студентов направления подготовки 10.03.01 «Информационная безопасность», профиль «Организация и технология защиты информации (на транспорте)»	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"

Э1	КонсультантПлюс - надежная правовая поддержка (http://www.consultant.ru)
Э2	Федеральная служба по техническому и экспортному контролю (https://fstec.ru/)
Э3	Федеральная служба безопасности Российской Федерации (http://www.fsb.ru/)
Э4	Среда электронного обучения BlackBoard Learn (https://bb.usurt.ru/)
Э5	Интернет портал ISO27000.RU (ЗАЩИТА-ИНФОРМАЦИИ.SU) (http://iso27000.ru)

6.3 Перечень информационных технологий, используемых при проведении практики, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

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	Операционная система Astra Linux
6.3.1.4	ESET NOD32 Antivirus
6.3.1.5	Платформа управления базами данных: SQL Server
6.3.1.6	Серверная операционная система: Windows Server
6.3.1.7	Abbyy FineReader
6.3.1.8	Adobe Acrobat
6.3.1.9	Система электронной поддержки обучения Blackboard Learn
6.3.1.10	Secret Net Studio
6.3.1.11	Система защиты информации от несанкционированного доступа: Dallas Lock
6.3.1.12	Linux Debian

6.3.2 Перечень информационных справочных систем и профессиональных баз данных

6.3.2.1	Автоматизированная система правовой информации на железнодорожном транспорте АСПИ ЖТ (профессиональная БД)
6.3.2.2	Консультант Плюс

7. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ПРОВЕДЕНИЯ ПРАКТИКИ

Назначение	Оснащение
База практики (Учебные аудитории для самостоятельной работы студентов, для проведения групповых и индивидуальных консультаций)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях
База практики (Для самостоятельной работы студентов)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, 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
Лаборатория "Программно-аппаратные средства защищенных информационных систем". Компьютерный класс - Учебная аудитория для	Специализированная мебель Лабораторное оборудование: Аппаратно-программный комплекс шифрования "Континент" Программно-аппаратный комплекс защиты информации ViPNet Custom, включающий в том числе киптографические средства" Оборудование для центра защиты информации, включающее в том числе интегрированную

проведения практических (занятий семинарского типа) и лабораторных занятий	систему безопасности "Рубеж", видеоохранную систему видеонаблюдения "Купол", аппартные средства аутетификации 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
База практики (Материальная техническая база профильной организации)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети Интернет Оборудование, используемое на объектах инфраструктуры ОАО "РЖД", в транспортных предприятиях и в сторонних организациях для конкретных видов работ
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
Учебная аудитория для проведения текущего контроля и промежуточной аттестации (Компьютерные классы)	Специализированная мебель Компьютерная техника с установленным лицензионным ПО, предусмотренным программой практики, с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду Университета

8. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ

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 практики, 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.
Обучающиеся в период практики:
- выполняют индивидуальные задания, предусмотренные программой практики;
- соблюдают правила внутреннего трудового распорядка;
- соблюдают требования охраны труда, техники безопасности и пожарной безопасности.
Выполнять самостоятельную работу и отчитываться по ее результатам студент должен в соответствии с утвержденным совместным планом (графиком) прохождения практики и формами отчетности. При выполнении самостоятельной работы и оформлении отчетных документов студент должен руководствоваться 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 СРС по темам практики в разделе 4 Программы практики "Содержание практики".