Приложение 4.1
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности
телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

профессионального модуля

УП.01 Эксплуатация информационно-телекоммуникационных систем и сетей

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНЫМ МОДУЛЯМ

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04. Обеспечение информационной безопасности телекоммуникационных систем в части освоения вида профессиональной деятельности (ВПД): эксплуатация информационно-телекоммуникационных систем и сетей и соответствующих профессиональных компетенций (ПК):

ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.3. Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.

ПК 1.4. Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.

Программа учебной практики является обязательной частью профессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики определяет содержание и объем знаний, умений, практического опыта которые предстоит приобрести в процессе прохождения практики, а также формирование общих и профессиональных компетенций. В период учебной практики осуществляется:

- практическое обучение студентов профессиональной деятельности;
- формирование умений, практического опыта, общих и профессиональных компетенций по специальности;
- воспитание сознательной трудовой и производственной дисциплины, уважения к трудовым традициям производственного коллектива.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и при повышении квалификации специалистов в области технической эксплуатации телекоммуникационных систем и информационно-коммуникационных сетей связи при наличии среднего общего образования.

Программа учебной практики УП.01 составлена для выполнения части практических занятий с целью освоения практического опыта, умений и знаний по МДК.01.01 Приемо-передающие устройства, линейные сооружения связи и источники электропитания и МДК 01.02 Телекоммуникационные системы и сети и МДК.01.03 Электрорадиоизмерения и метрология.

Общий объем учебной практики составляет 108 часов.

Рабочая программа разработана для очной формы обучения.

Перечень профессиональных компетенций ПМ.01

Результатом освоения программы производственной практики является овладение обучающимися видом профессиональной деятельности (ВПД): эксплуатация информационно-телекоммуникационных систем и сетей необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименование результата обучения**
ПК.1.1	Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей.
ПК.1.2	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей.

ПК.1.3.	Проводить техническое обслуживание оборудования информационно-телекоммуникационных систем и сетей.
ПК.1.4.	Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей.
ОК.1	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК.2	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК.3	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК.4	. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК.9	Использовать информационные технологии в профессиональной деятельности.
ОК.10	Пользоваться профессиональной документацией на государственном и иностранном языке.

Цели и планируемые результаты освоения

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе прохождения учебной практики должен:

Иметь практический опыт в:

- монтаже, настройке, проверке функционирования и конфигурировании оборудования ИТКС;
- текущем контроле функционирования оборудования ИТКС;
- проведениитехническогообслуживания,диагностикетехническогосостояния, поиске неисправностей и ремонте оборудования ИТКС.

уметь:

- осуществлять техническую эксплуатацию линейных сооружений связи;
- производить монтаж кабельных линий и оконечных кабельных устройств;
- настраивать, эксплуатировать и обслуживать оборудование ИТКС;
- осуществлять подключение, настройку мобильных устройств и распределенных сервисов ИТКС;
- производить испытания, проверку и приемку оборудования ИТКС;
- проводить работы по техническому обслуживанию, диагностике технического состояния и ремонту оборудования ИТКС.

знать:

- принципы построения и основных характеристик информационно - телекоммуникационных систем и сетей (далее - ИТКС);
-принципы передачи информации в ИТКС;
-виды и характеристики сигналов в ИТКС;
-виды помех в каналах связи ИТКС и методы защиты от них;
-разновидности линий передач, конструкции характеристики электрических и оптических кабелей связи;
-технологии и оборудование удаленного доступа в ИТКС;

- принципы построения, основные характеристики активного сетевого и коммуникационного оборудования ИТКС.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Тематический план учебной практики
ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

Код ПК	Кодинаименования профессионального модуля, код и наименованиеМДК	Кол-вочасовна учебную практику по ПМ и соответствующим МДК	Видыработ	Наименованиятемучебной практики	Кол-во часов по темам
1	2	3	4	5	6
ПМ.01Техническаяэксплуатацияинфокоммуникационныхсетейсвязи					
ПК1.1 ПК1.2	**МДК.01.01**Приемо-передающие устройства, линейные сооруженияисвязии источники электропитания	18	ИсследованиенестабильностичастотыАГсобранных на CL элементах с кварцевой стабилизацией частоты	Тема1.1Технологиямонтажа радиопередающих устройств	9
			Исследованиеумножителячастотырадиопередатчика.		
			Регулировкаинастройкаусилителейрадиочастоты		
			Исследованиеодноконтурнойвходнойцепи.	Тема2.1Технологиямонтажа радиоприемных устройств	9
			Исследование эффектов многосигнальной избирательностирадиоприемника.Измерение коэффициентаусиленияодетекторноготрактав отсутствии помех.		
			Исследованиетрактапромежуточнойчастоты радиоприемника.		
			Исследованиечастотногодетектораавтогенераторас частотноймодуляцией.Детекторнаяхарактеристика.		
		36	МонтажНЧкабелейхолоднымметодом	**Тема3.4.**Прокладкаимонтаж оборудования линейной части сети квантовыхкоммуникаций	24
			МонтажВЧкабелейхолоднымметодом.		
			Монтажоптическихкабелей		
			МонтажКРТП-В.	**Тема3.2.**Оконечныекабельные устройствадляэлектрическихи волоконно-оптических кабелей	12
			Определениевидаиместаповреждениякабельной линии с помощью прибора «Гамма-люкс»		

			Оформлениедокументациипристачелинииэксплуатацию	связи	
ПК1.3 ПК1.4	**МДК.01.02 Телекоммуникационные системы и сети**	12	УстройствоGSMсетей,ихприѐмникови передатчиков.Измерения уровнейсигналови алгоритмы выбора базовых станций.	Тема.2.2Системысотовой подвижной радиосвязи	12
			Видыантенниихэффективность.Приѐмсигналов базовых станций, демодуляция и декодирование.		
ПК1.3 ПК1.4		42	Нормирование параметров ОЦК и групповых цифровых трактов. ОЦК и групповые цифровые тракты. Нормирование параметров. Выбор измерительных приборов. Методика измерений параметровцифровыхканаловитрактов.Анализ результатов измерений.	**Тема3.1.**Монтаж,настройкаи эксплуатация оборудования цифровых систем передачи	18
			Разделкакабелейс«витойпарой»длявключенияв коннекторы соответствующей емкости. Монтаж коммутационныхпанелей.		
			ОборудованиеМПСуперТел.Назначение,основные технические данные, состав оборудования. Структурныесхемыосновныхузловоборудования. Структуравременногоцикла.Программное обеспечение «СуперТел».		
			Организациясвязиспримененией технологии ADSL, G.SHDSL. Организация связи с применениемтехнологии BPON	**Тема3.2.**Монтаж,первичная инсталляция, мониторинг оборудованияпроводного цифрового доступа	12
			Конфигурация оборудования BPONTERAWAVE с использованием системы управления программного обеспечения		
			Организациясвязиспримененией технологии SDH. Конфигурирование SDH-услуг. Создание подсети резервирования. Конфигурирование услуг передачи тональных сигналов и данных. Загрузка STM-1 потока E1. КонфигурацияоборудованияSTM-1(METRO500).	**Тема3.3.**Инсталляция,настройка и эксплуатация оборудования волоконно-оптических систем передачинабазетехнологииSDH	6
			КонфигурированияуслугсетиEthernet.Конфигурирование	**Тема3.4.** Инсталляция,	6

			услугсетиGigabitEthernet.Конфигурацияуслугсети 10M/100MEthernet. Установка транзитногоилитерминальногозаголовкаVC-4. Конфигурация интерфейса.	настройкаиэксплуатация оборудования ВОСП технологии WDM	
ВСЕГО часов	108				

Содержание учебной практики

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

Код и наименование профессиональногомодуля, МДКитемучебнойпрактики	**Содержаниеучебныхзанятий**		**Объемчасов на учебную практику**		**Уровень освоения**
1	**2**		Обяз. часть	Вар. часть	**4**
ПМ.01Эксплуатацияинформационно-телекоммуникационныхсистемисетей					
МДК.01.01Приемо-передающиеустройства,линейныесооруженияисвязиииточникиэлектропитания			**54**		
Тема1. Прокладка и монтаж направляющихсистемпередачи Тема 2 Оконечные кабельные устройствадляэлектрическихи волоконно-оптических кабелей связи	**Содержание**				
	1	Исследование нестабильности частоты АГ собранных на CL элементах с кварцевой стабилизацией частоты	3	-	2
	2	Исследованиеумножителячастотырадиопередатчика.	3	-	
	3	Регулировкаинастройкаусилителейрадиочастоты	3	-	
	4	Исследованиеодноконтурнойвходнойцепи.Исследованиетракта промежуточной частоты радиоприемника.	-	3	
	5	Исследованиеэффектовмногосигнальнойизбирательности радиоприемника.Измерениекоэффициентаусиленияодетекторного тракта в отсутствии помех.	-	3	
	6	Исследованиечастотногодетектораавтогенераторасчастотной модуляцией. Детекторная характеристика.	3	-	
	7	МонтажНЧкабелейхолоднымметодом	-	6	
	8	МонтажВЧкабелейхолоднымметодом.	-	6	
	9	Монтажоптическихкабелей	-	6	
	10	МонтажКРТП-В.	-	6	
	11	Определениевидаиместаповреждениякабельнойлинииспомощью	-	6	

		прибора«Гамма-люкс»			
МДК.01.02Телекоммуникационныесистемыисети			2		
	1	УстройствоGSMсетей,ихприѐмниковипередатчиков.Измерения уровней сигналов и алгоритмы выбора базовых станций.	6	-	
	2	Видыантенниихэффективность.Приѐмсигналовбазовыхстанций, демодуляция и декодирование.	6	-	
	3	Нормирование параметров ОЦК и групповых цифровых трактов. ОЦК и групповые цифровые тракты. Нормирование параметров. Выбор измерительных приборов.Методикаизмеренийпараметровцифровыхканаловитрактов.Анализ результатов измерений.	6	-	2
	4	Разделкакабелейс«витойпарой»длявключениявконнекторы соответствующей емкости. Монтаж коммутационных панелей.	6	-	
	5	ОборудованиеМПСуперТел.Назначение,основныетехническиеданные,состав оборудования. Структурные схемы основных узлов оборудования. Структура временногоцикла.Программноеобеспечение«СуперТел».	6	-	
	6	Организациясвязиспримененией технологииADSL,G.SHDSL.Организация связи с применением технологии BPON	6	-	
	7	КонфигурацияоборудованияBPONTERAWAVEиспользованиемсистемы управления программного обеспечения	6	-	
	8	Организациясвязиспримененией технологииSDH.КонфигурированиеSDH- услуг. Создание подсети резервирования. Конфигурированиеуслугпередачитональныхсигналовиданных.Загрузка STM-1 потока E1.Конфигурация оборудования STM-1 (METRO 500).	6	-	
	9	КонфигурированияуслугсетиEthernet.КонфигурированиеуслугсетиGigabit Ethernet. Конфигурация услуг сети 10M/100M Ethernet. Установка транзитного или терминального заголовка VC-4. Конфигурация интерфейса.	6	-	
Всего часов:	108				

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Учебная практика профессионального модуля ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей связи по профилю специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит «лаборатория технических средств информатизации. Программных и программно – аппаратных средств защиты информации», оснащенная необходимым для реализации программы практики оборудованием.

Оборудование кабинета: рабочее место преподавателя; рабочие места обучающихся, доска аудиторная, мультимедийное оборудование, системный блок, монитор.

Программное обеспечение:

Простая (неисключительная) лицензия на Программное обеспечение «Рубикон» - комплекс межсетевого экранирования и средство обнаружения вторжений
Простая (неисключительная) лицензия на Программное обеспечение «Сканер-ВС»
Простая (неисключительная) лицензия на Программное обеспечение «Программное обеспечение KOMRAD Enterprise SIEM»
Неискл. право DallasLock 8.0-K (СЗИ НСД, СКН, МЭ, СОВ, МП, РК, СКН2) (для обучения)
Неискл. право DallasLock ЕЦУ 3 устройства (для обучения)
Неискл. право DallasLockLinux (СЗИ НСД, СКН) (для обучения)
Несертифицированный комплект для установки DallasLock 8.0-K (для обучения)
Несертифицированный комплект для установки DallasLockLinux (для обучения)
Право на использование модулей защиты от НСД и контроля устройств средства защиты информации SecretNetStudio 8
Право на использование модулей защиты диска и шифрования контейнеров средства защиты информации SecretNetStudio 8
Право на использование модуля персонального межсетевого экрана средства защиты информацииSecretNetStudio 8
Право на использование комплекта «Постоянная защита» Средства защиты информации SecretNetStudio LSP
Право на использование Средства защиты информации vGate R2 EnterprisePlus (за 1 физический процессор на защищаемом хосте)
Программный комплекс ViPNetAdministrator 4
Лицензия на 6 месяцев для ПО ViPNetAdministrator 4 (для обучения)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 1-янода) (для образовательных учреждений)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 2-янода) (для образовательных учреждений)
Модуль AdvancedThreatProtection на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль MailSecurity на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль StreamAntivirus на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Лицензия на 1 год для UserGateLogAnalyzer (для образовательных учреждений)
Сенсор для подключения UserGateLogAnalyzer до 5 пользователей (для образовательных учреждений)
Лицензия UserGateManagementCenter на 1 год (для образовательных учреждений)
Сенсор для подключения UserGateManagementCenter до 5 пользователей (для образовательных учреждений)

Учебно-методические пособия:
Учебное пособие по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторная (практическая) работа по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)

Материалы слайдов по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторный стенд (программный продукт) по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (в виде образов виртуальных машин)
Учебное пособие: «Безопасность КИИ»
Учебное пособие: «Программно-аппаратный комплекс ViPNetxFirewall»
Учебное пособие: «Технология построения VPN ViPNet. Курс лекций»
Учебное пособие: «Программно-аппаратные комплексы ViPNet HW 4»
Учебное пособие: «Администрирование системы защиты информации ViPNet версии 4»
Учебное пособие «Администрирование ViPNetLinuxCoordinator»
Учебное пособие: «Основы безопасности операционной системы AstraLinuxSpecialEdition. Управление доступом»

Информационное обеспечение реализации программы

1. Волчков, А. Б. Цифровые системы передачи. Разработка цифровой системы передачи и организация транспортной сети: учебно-методическое пособие по выполнению курсового проектирования :учебно-методическое пособие / А. Б. Волчков, М. В. Лобастова,А. Ю. Матюхин. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2021. — 54 с. — Текст :электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/180187— Режим доступа: для авториз. пользователей.
2. Крухмалев В. В. Цифровые системы передачи: Учебное пособие для вузов – 2-е изд., перераб.и доп. / В.В. Крухмалев, В.Н. Гордиенко, А.Д. Моченов. - Москва : Горячая Линия–Телеком, 2018. - 376 с. - ISBN 978-5-9912-0226-8. - URL: http://m.ibooks.ru/bookshelf/333998/reading - Текст: электронный.
3.Скляров,О.К.Волоконно-оптическиесетиисистемысвязи:учебное пособие/О.К.Скляров. — 4-е изд., стер. — Санкт-Петербург : Лань, 2018. — 268 с. — ISBN 978-5-8114-1028-6. — Текст : электронный// Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/104959
— Режимдоступа:дляавториз.пользователей.
Сетиителекоммуникации :учебникипрактикумдлясреднегопрофессиональногообразования/ К. Е. Самуйлов [и др.] ; под редакциейК. Е. Самуйлова,И. А. Шалимова,Д. С. Кулябова. —Москва : Издательство Юрайт, 2022. — 363 с. — (Профессиональное образование). — ISBN 978-5- 9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495353
4.Телекоммуникационные сети и технологии : учебное пособие / Х. Ш. Кульбикаян, Б. Х. Кульбикаян, А. В.Дицков, А. В. Шандыбин ; подредакциейХ.Ш. Кульбикаяна. —Ростов-на-Дону: РГУПС, 2019. — 212 с. — ISBN 978-5-88814-869-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/134039— Режим доступа: для авториз. пользователей.
5. Пушкарѐв, В. П. Радиоприемные устройства : учебник / В. П. Пушкарѐв. — Москва :Ай Пи Ар Медиа, 2021. — 226 с. — ISBN 978-5-4497-0181-7. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/105788 (дата обращения: 27.09.2022.
6. Никитин, Н. П. Устройства приема и обработки сигналов. Системы управления приемником. Устройства борьбы с помехами : учебное пособие для СПО / Н. П. Никитин, В. И. Лузин ; под редакцией В. И. Гадзиковского. — 2-е изд. — Саратов, Екатеринбург : Профобразование, Уральский федеральный университет, 2019. — 87 с. — ISBN 978-5-4488-0478-6, 978-5-7996-2888-8. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87887 (дата обращения: 27.09.2022).
7. Ходасевич О.Р. Информационные кабельные сети / О.Р. Ходасевич. - Минск : РИПО, 2019. - 194 с. - ISBN 978-985-503-860-4. - URL: https://ibooks.ru/bookshelf/361839/reading (дата обращения: 29.09.2022). - Текст: электронный
Пушкарѐв, В. П. Радиоприемныеустройства: учебник / В. П. Пушкарѐв. — Москва :АйПиАр Медиа, 2021. — 226 с. — ISBN 978-5-4497-0181-7. — Текст : электронный // Электронный ресурс

цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/105788 (дата обращения: 27.09.2022.
8. Никитин, Н. П. Устройства приема и обработки сигналов. Системы управления приемником. Устройства борьбы с помехами : учебное пособие для СПО / Н. П. Никитин, В. И. Лузин ; под редакцией В. И. Гадзиковского. — 2-е изд. — Саратов, Екатеринбург :Профобразование,Уральский федеральный университет, 2019. — 87 c. — ISBN 978-5-4488-0478-6, 978-5-7996-2888-8.
9. Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87887 (дата обращения: 27.09.2022).
ОИЗ. Ходасевич О.Р. Информационные кабельные сети / О.Р. Ходасевич. - Минск : РИПО, 2019. - 194 с. - ISBN 978-985-503-860-4. - URL: https://ibooks.ru/bookshelf/361839/reading (дата обращения: 29.09.2022). - Текст: электронный.

Дополнительные источники

1. Зикий, А. Н. Передатчики помех современным средствам связи : учебное пособие / А. Н. Зикий, А. В. Помазанов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 176 с. — ISBN 978-5-9275-3653-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/115524 (дата обращения: 27.09.2022).
2. Ходасевич О.Р. Информационные кабельные сети / О.Р. Ходасевич. - Минск : РИПО, 2019. - 194 с. - ISBN 978-985-503-860-4. - URL: https://ibooks.ru/bookshelf/361839/reading (дата обращения: 29.09.2022). - Текст: электронный
3. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования /К. Е. Самуйлов[идр.] ;подредакциейК. Е. Самуйлова,И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495353(дата обращения: 29.09.2022)
4. Зикий, А. Н. Передатчики помех современным средствам связи : учебное пособие / А. Н. Зикий, А. В. Помазанов. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 176 с. — ISBN 978-5-9275-3653-5. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/115524 (дата обращения: 27.09.2022).
5. Ходасевич О.Р. Информационные кабельные сети / О.Р. Ходасевич. - Минск : РИПО, 2019. - 194 с. - ISBN 978-985-503-860-4. - URL: https://ibooks.ru/bookshelf/361839/reading (дата обращения: 29.09.2022). - Текст: электронный
6. Сети и телекоммуникации : учебник и практикум для среднего профессионального образования /К. Е. Самуйлов[идр.] ;подредакциейК. Е. Самуйлова,И. А. Шалимова, Д. С. Кулябова. — Москва : Издательство Юрайт, 2022. — 363 с. — (Профессиональное образование). — ISBN 978-5-9916-0480-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495353(дата обращения: 29.09.2022)

Электронные ресурсы

1.Ассоциация документальной электросвязи [электронный ресурс] : [официальный сайт].– Режим доступа: http://www.rans.ru
2.Comnews.ru. Новости телекоммуникаций, вещание и ИТ [Электронный ресурс]: [независимое сетевое СМИ]. – Режим доступа: www. comnews.ru (Новости России и СНГ в сфере мобильной, беспроводной, спутниковой, фиксированной связи, интернета, кабельных сетей и других видов телекоммуникаций и информационных технологий).
3.Руководство по строительству линейных сооружений местных сетей связи [Электронный ресурс]: учебное пособие. – Режим доступа: http://vsesnip.com/Data1/44/44551/index.htm.
ЭР4.Руководство по строительству линейных сооружений местных сетей связи (часть 2) [Электронный ресурс]. – Режим доступа: http://www.izmer-ls.ru/srek.html.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения практики и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

При оценивании отчета по практике учитываются оценка уровня прохождения учебной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Кодинаименование профессиональных компетенций, формируемыхврамках модуля	Критериоценки	Методыоценки
ПК1.1.Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей ПК1.2.Осуществлять диагностику техническогосостояния, поиск неисправностей и ремонт оборудования информационно-телекоммуникационных систем и сетей. ПК1.3.Проводить техническое обслуживание оборудования информационно - телекоммуникационных систем и сетей. ПК1.4.Осуществлять контроль функционирования информационно-телекоммуникационных систем и сетей	ОПОР 1. Производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; ОПОР 2. Проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; ОПОР3.Измерятьосновныепоказателии характеристикипривыполненииработпонастройке, проверке функционирования и конфигурирования ИТКС. ОПОР 4. Осуществлять техническую эксплуатацию линейных сооружений связи; ОПОР 5.Проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; ОПОР 6. Измерять основные параметры и характеристикипривыполненииработпо диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС. ОПОР7.Осуществлятьтехническуюэксплуатацию линейных сооружений ИТКС; ОПОР8.Измерятьосновныепараметрыи характеристикипривыполнениитехнического обслуживанияоборудования ИТКС; ОПОР9.Производитьконтрольирегулировку основных параметров источников питания оборудования ИТКС. ОПОР10.Проводитьмониторингиконтроль функционирования оборудования ИТКС; ОПОР11.Измерятьосновныепараметрыи характеристики оборудования ИТКС; ОПОР12.Вестиэксплуатационно-техническую документацию на оборудование ИТКС.	**Текущийконтрольв форме:** -формализованного наблюденияовремя выполнениязаданий; -проведения анализа практическихзанятий -тестирования; - формализованного наблюденияпреподавателя за выполнением конкретного задания; -дифференцированные зачеты по учебной и производственной практике. **Промежуточный контрольвформе:** –дифференцированный зачет по УП.

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.2
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности
телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

профессионального модуля

УП.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНЫМ МОДУЛЯМ

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики является обязательной частью профессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики определяет содержание и объем знаний, умений, практического опыта которые предстоит приобрести в процессе прохождения практики, а также формирование общих и профессиональных компетенций. В период учебной практики осуществляется:

- практическое обучение студентов профессиональной деятельности;
- формирование умений, практического опыта, общих и профессиональных компетенций по специальности;
- воспитание сознательной трудовой и производственной дисциплины, уважения к трудовым традициям производственного коллектива.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и при повышении квалификации специалистов в области технической эксплуатации телекоммуникационных систем и информационно-коммуникационных сетей связи при наличии среднего общего образования.

Программа учебной практики УП.02 составлена для выполнения части практических занятий с целью освоения практического опыта, умений и знаний по МДК.02.01 Защита информации в информационно- телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты и МДК.02.02 Криптографическая защита информации.

Общий объем учебной практики составляет 72 часов.

Рабочая программа разработана для очной формы обучения.

Перечень профессиональных компетенций ПМ.02

Результатом освоения программы производственной практики является овладение обучающимися видом профессиональной деятельности (ВПД): эксплуатация информационно-телекоммуникационных систем и сетей необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности профессиональных компетенций
ВД 2.	Защитаинформациивинформационно-телекоммуникационныхсистемахисетяхс использованием программных и программно-аппаратных, в том числе криптографических средств защиты
ПК 2.1	Производитьустановку,настройку,испытанияиконфигурированиепрограммныхи программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживатьбесперебойнуюработупрограммныхипрограммно-аппаратных,в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальныхвоздействийвинформационно-телекоммуникационныхсистемахи сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работатьвколлективеикоманде,эффективновзаимодействоватьсколлегами,руководством, клиентами.
ОК 09.	Использоватьинформационныетехнологиивпрофессиональнойдеятельности.
ОК 10.	Пользоватьсяпрофессиональнойдокументациейнагосударственномииностранном языках.

Цели и планируемые результаты освоения

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе прохождения учебной практики должен:

Иметь практический опыт в	установке, настройке, испытаниях и конфигурировании про- граммных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, втом числе криптографических средств защиты в соответствии с предъявляемыми требованиями.
уметь	выявлять и оценивать угрозы безопасности информации в ИТКС;У2 настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить конфигурирование программных и программно- аппаратных, в том числе криптографических средств защиты информа- ции; проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить восстановление процесса и параметров функционирова- ния программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	возможныеугрозыбезопасностиинформациивИТКС; способызащитыинформациионтнесанкционированногодоступа (далее - НСД) и специальных воздействий на нее; типовые программные и программно-аппаратные средства защиты информациивинформационно-телекоммуникационныхсистемахисе- тях; криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; порядоктестированияфункцийпрограммныхипрограммно-аппаратных, в том числе криптографических средств защиты информации;

	организациюисодержаниетехническогообслуживанияиремонта программно-аппаратных, в том числе криптографических средств защиты информации; порядок и правила ведения эксплуатационной документации на программныеипрограммно-аппаратные, в том числе криптографические средства защиты информации.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Код ПК	Код и наименования профессионального модуля, код и наименование МДК	Количество часов на учебную практику по ПМ и соответствующим МДК	Видыпрактическойподго - товки	Наименования тем учебной практики	Количество часов по темам		
					Общая	обязат. часть	вариати в. часть
ПК2.1 ПК2.2 ПК2.3	ПМ.02Защита информации в информационно-телекоммуникацион- ных системах и сетях с использованиемпро- граммныхи программ- но-аппаратных, в том числе криптографических средствзащитыМДК02.01 Защита информациив информационно-телекомму- никационных систе- махисетях с использованием про-граммныхи программ- но-аппаратных средств за- щиты МДК 02.02 Криптографическая	108	- Выбор,подключение,настройкамежсетевогоэкрана. - Администрирование межсетевого экрана. - Ознакомление, подключение,настройкасистемы резервного копирования - Администрированиесистемы резервного копирования. - Ознакомление, подключение,настройкасистемы антивирусной защиты. - Администрирование системы антивирусной защиты. - Проведениеинструктажа по технике безопасности. - Составлениеалгоритма хеш-функции - Составлениеалгоритма шифра	Тема1.Выявлениеразличия характеристик различных алгоритмов шифрования	10	10	5
				Тема2.Выявлениеобщих характеристик различных алгоритмов шифрования	10	10	5
				Тема 3. Исследование передачи информации по зашифрованному каналу	9	9	5
				Тема 4. Исследование передачи информации по незашифрованному каналу	8	8	6
				Тема 5. Оценка эффективность применения различных алгоритмов.	9	9	5
				Тема6. Настройка системы антивирусной защиты	9	9	6
				Тема7.Использованиемежсетевого экрана для защиты от несанкционированного доступа	8	8	5

	защита ин-формации			Тема8.Системы резервного копирования	9	9	6
	ВСЕГО часов	72			72	72	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Учебная практика профессионального модуля ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты по профилю специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит «лаборатория технических средств информатизации. Программных и программно – аппаратных средств защиты информации», оснащенная необходимым для реализации программы практики оборудованием.

Оборудование кабинета: рабочее место преподавателя; рабочие места обучающихся, доска аудиторная, мультимедийное оборудование, системный блок, монитор.

Программное обеспечение:

Простая (неисключительная) лицензия на Программное обеспечение «Рубикон» - комплекс межсетевого экранирования и средство обнаружения вторжений
Простая (неисключительная) лицензия на Программное обеспечение «Сканер-ВС»
Простая (неисключительная) лицензия на Программное обеспечение «Программное обеспечение KOMRAD Enterprise SIEM»
Неискл. право DallasLock 8.0-K (СЗИ НСД, СКН, МЭ, СОВ, МП, РК, СКН2) (для обучения)
Неискл. право DallasLock ЕЦУ 3 устройства (для обучения)
Неискл. право DallasLockLinux (СЗИ НСД, СКН) (для обучения)
Несертифицированный комплект для установки DallasLock 8.0-K (для обучения)
Несертифицированный комплект для установки DallasLockLinux (для обучения)
Право на использование модулей защиты от НСД и контроля устройств средства защиты информации SecretNetStudio 8
Право на использование модулей защиты диска и шифрования контейнеров средства защиты информации SecretNetStudio 8
Право на использование модуля персонального межсетевого экрана средства защиты информацииSecretNetStudio 8
Право на использование комплекта «Постоянная защита» Средства защиты информации SecretNetStudio LSP
Право на использование Средства защиты информации vGate R2 EnterprisePlus (за 1 физический процессор на защищаемом хосте)
Программный комплекс ViPNetAdministrator 4
Лицензия на 6 месяцев для ПО ViPNetAdministrator 4 (для обучения)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 1-янода) (для образовательных учреждений)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 2-янода) (для образовательных учреждений)
Модуль AdvancedThreatProtection на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль MailSecurity на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль StreamAntivirus на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Лицензия на 1 год для UserGateLogAnalyzer (для образовательных учреждений)
Сенсор для подключения UserGateLogAnalyzer до 5 пользователей (для образовательных учреждений)
Лицензия UserGateManagementCenter на 1 год (для образовательных учреждений)
Сенсор для подключения UserGateManagementCenter до 5 пользователей (для образовательных учреждений)

Учебно-методические пособия:
Учебное пособие по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)

Лабораторная (практическая) работа по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Материалы слайдов по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторный стенд (программный продукт) по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (в виде образов виртуальных машин)
Учебное пособие: «Безопасность КИИ»
Учебное пособие: «Программно-аппаратный комплекс ViPNetxFirewall»
Учебное пособие: «Технология построения VPN ViPNet. Курс лекций»
Учебное пособие: «Программно-аппаратные комплексы ViPNet HW 4»
Учебное пособие: «Администрирование системы защиты информации ViPNet версии 4»
Учебное пособие «Администрирование ViPNetLinuxCoordinator»
Учебное пособие: «Основы безопасности операционной системы AstraLinuxSpecialEdition. Управление доступом»

Информационное обеспечение реализации программы

1 Бабаш, А. В. Криптографические методы защиты информации. Том 1 : учебно-методическое пособие/А.В.Бабаш.—2-еизд.,перераб.идоп.—Москва:РИОР:ИНФРА-М,2021.—413с.
— (Высшее образование: Бакалавриат). - ISBN 978-5-369-01267-3. - Текст : электронный. - URL:https://znanium.com/catalog/product/1215714
2 Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова.— Москва : РТУ МИРЭА, 2021. — 172 с.— Текст: электронный// Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563
3Маршаков, Д. В. Методы и средства криптографической защиты информации. Практическийкурс:учебноепособие/Д.В.Маршаков,Д.В.Фахти.—Москва:ИНФРА-М,2022.
— 76 с. — (Высшее образование). - ISBN 978-5-16-110842-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1891129
4 Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 352 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-557-8. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189341
5. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2022. — 592 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-8199-0730-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1843022

Электронные ресурсы

1. CIT-Forum:Центринформационныхтехнологий:материалысайта[Электронныйресурс]. - Режим доступа: http://citforum.ru/, свободный.
2. Библиотека учебных курсов/ Интернет-Университет информационных технологий - Интуит (Национальный Открытый университет) [Электронный ресурс]. - Режим доступа: http://old.intuit.ru/catalog/, свободный.
3. Материалы Microsoft Virtual Academy [Электронный ресурс]. - Режим доступа: https://www.microsoftvirtualacademy.com/Home.aspx, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения практики и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

При оценивании отчета по практике учитываются оценка уровня прохождения учебной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК2.1.Производить установку, настрой-ку, испытания и конфигурирование программных и про-граммно-аппаратных, в том числекриптографи-ческих средств за-щиты информации от несанкциониро-ванного доступа и специальныхвоз-действийвоборудо-вание информаци-онно-телекоммуникационн ых систем и сетей.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить установку и на- стройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; проводить конфигурирование программных и программно- аппаратных (в том числе крипто- графических) средств защиты информации;	**Текущий контроль в форме:** - защитызаданийпоучебно йпрактике; - наблюденияиоценкив ыполненияработ по учебной практике; - наблюденияпреподав ателязавыполне- нием конкретного задания. **Промежуточный контроль в форме:** комплексныйдифференц ированныйзачет по учебной практике, производственной практике.
ПК 2.2. Поддержи-ватьбесперебойную работупрограммных и программно-аппаратных, в том числе криптографи-ческих средств за-щиты информации в информационно-телекоммуникаци-онных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе крипто- графических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и про- граммно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт программно- аппаратных (в том числе крипто-графических) средств защиты информации;	**Текущий контроль в форме:** - защитызаданийпоучебно йпрактике; - наблюденияиоценкив ыполненияработ по учебной практике; - наблюденияпреподав ателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференци рованныйзачет по учебной практике, производственной практике.

ПК 2.3. Осуществлять защиту информации от несанкционированныхдействий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программныхи программно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно- аппаратных (в том числе крипто- графических) средств защиты информации;	**Текущий контроль в форме:** - защитызаданийпоучебной практике; - наблюденияиоценкивыполненияработ по учебной практике; - наблюденияпреподавателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференцированныйзачет по учебной практике, производственной практике.

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно- программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.3
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности
телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

профессионального модуля

УП.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНЫМ МОДУЛЯМ

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики является обязательной частью профессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики определяет содержание и объем знаний, умений, практического опыта которые предстоит приобрести в процессе прохождения практики, а также формирование общих и профессиональных компетенций. В период учебной практики осуществляется:

- практическое обучение студентов профессиональной деятельности;
- формирование умений, практического опыта, общих и профессиональных компетенций по специальности;
- воспитание сознательной трудовой и производственной дисциплины, уважения к трудовым традициям производственного коллектива.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и при повышении квалификации специалистов в области технической эксплуатации телекоммуникационных систем и информационно-коммуникационных сетей связи при наличии среднего общего образования.

Программа учебной практики УП.03 составлена для выполнения части практических занятий с целью освоения практического опыта, умений и знаний по МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты и МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей.

Общий объем учебной практики составляет 72 часов.

Рабочая программа разработана для очной формы обучения.

Перечень профессиональных компетенций ПМ.03

Результатом освоения программы производственной практики является овладение обучающимися видом профессиональной деятельности (ВПД): эксплуатация информационно-телекоммуникационных систем и сетей необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности профессиональных компетенций
ВД 3.	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим канала в информационно-телекоммуникационных системах и сетях
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работатьвколлективеикоманде,эффективновзаимодействоватьсколлегами,руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 09.	Использоватьинформационныетехнологиивпрофессиональнойдеятельности.

Цели и планируемые результаты освоения

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе прохождения учебной практики должен:

Иметь практический опыт в	- в установке, монтаже, настройке и испытаниях технических средств защиты информации от утечки по техническим каналам; - защите информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями; - проведении отдельных работ по физической защите линий связи информационно-телекоммуникационных систем и сетей.
уметь	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; использовать средства физической защиты линий связи ИТКС; применять нормативные правовые акты и нормативные методические документы в области защиты информации.
знать	способызащитыинформациииотутечкипотехническимканаламс использованием технических средств защиты; основныетипытехническихсредствзащитыинформациииотутечки по техническим каналам; методики измерения параметров побочных электромагнитных излученийинаводок(далее-ПЭМИН),атакжепараметровфоновыхшумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; организациюиосодержаниетехническогообслуживанияиремонта технических средств защиты информации от утечки по техническим каналам; порядокиправиларведенияэксплуатационнойдокументациинатехнические средства защиты информации от утечки по техническим каналам; содержаниеиорганизациюработпофизическойзащителинийсвязи ИТКС; принципыдействияиосновныехарактеристикитехническихсредств физической защиты; законодательство в области информационной безопасности, структуругосударственнойсистемызащитыинформации,нормативныхпра-

	вовых актов уполномоченных органов исполнительной власти, национальных стандартов и других методических документов в области информационной безопасности; принципы и методы организационной защиты информации, организационного обеспечения информационной безопасности в организациях.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Тематический план учебной практики
ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Код ПК	**Код, наименование профессиональных модулей, наименования разделов профессионального модуля**	**Кол-во часов**	**Виды работ**	**Наименования тем учебной практики**	**Кол-во часов по темам**
1	***2***	***3***	***4***	***5***	***6***
	ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	36			
ПК 3.1-ПК.3.4 ОК 1 – ОК 7, ОК 9	МДК.03.01Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	18	Получение первоначальных практических умений по защите информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	Тема 1.1.Технические каналы утечки информации	12
				Тема 1.2Эксплуатация технических средств защиты информации	6
ПК 3.5 ОК 1 – ОК 7, ОК 9	МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей	12	Получение первоначальных практических умений по физической защите линий связи ИТКС	Тема 2.1.Применение инженерно-технических средств физической защиты	6
				Тема 2.2. Эксплуатация инженерно-технических средств физической защиты	6
	Промежуточная аттестация в форме диф.зачета				6

Содержание учебной практики

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Код, наименование профессиональных модулей, наименование разделов профессионального модуля и тем учебной практики	**Содержание занятий учебной практики**	**Объем часов**
1	***2***	***3***
ПМ03.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты		**36**
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**18**
Тема 1.1.Технические каналы утечки информации	Содержание	12
	Расчет наводок в каналах связи. Побочные электромагнитные излучения ПК. Восстановление информации при перехвате ПЭМИН. Съем информации по электрическим каналам утечки информации.	
Тема 1.2. Эксплуатация технических средств защиты информации	Содержание	6
	Установка и настройка технических средств защиты информации. Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации. Проведение аттестации объектов информатизации.	
Раздел 2. Физическая защита линий связи ИТКС		**12**
Тема 2.1. Применение инженерно-технических средств физической защиты	Содержание	6
	Рассмотрение системы контроля и управления доступом. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. Рассмотрение датчиков периметра, их принципов работы. Выполнение звукоизоляции помещений системы зашумления.	

Тема 2.2 Эксплуатация инженерно-технических средств физической защиты	Содержание	6
	Технические средства защиты информации в телефонных линиях Технические средства обнаружения, локализации средств негласного получения информации. Нейтрализация радиоизлучающих специальных технических. Акустические и виброакустические каналы утечки. Исследование оптоэлектронного канала утечки информации. Технические средства защиты от утечек информации по проводным линиям.	
Промежуточная аттестация в форме зачета/дифференцированного зачета		6

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Учебная практика профессионального модуля ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты по профилю специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит «лаборатория технических средств информатизации. Программных и программно – аппаратных средств защиты информации», оснащенная необходимым для реализации программы практики оборудованием.

Оборудование кабинета: рабочее место преподавателя; рабочие места обучающихся, доска аудиторная, мультимедийное оборудование, системный блок, монитор.

Программное обеспечение:

Простая (неисключительная) лицензия на Программное обеспечение «Рубикон» - комплекс межсетевого экранирования и средство обнаружения вторжений
Простая (неисключительная) лицензия на Программное обеспечение «Сканер-ВС»
Простая (неисключительная) лицензия на Программное обеспечение «Программное обеспечение KOMRAD Enterprise SIEM»
Неискл. право DallasLock 8.0-K (СЗИ НСД, СКН, МЭ, СОВ, МП, РК, СКН2) (для обучения)
Неискл. право DallasLock ЕЦУ 3 устройства (для обучения)
Неискл. право DallasLockLinux (СЗИ НСД, СКН) (для обучения)
Несертифицированный комплект для установки DallasLock 8.0-K (для обучения)
Несертифицированный комплект для установки DallasLockLinux (для обучения)
Право на использование модулей защиты от НСД и контроля устройств средства защиты информации SecretNetStudio 8
Право на использование модулей защиты диска и шифрования контейнеров средства защиты информации SecretNetStudio 8
Право на использование модуля персонального межсетевого экрана средства защиты информацииSecretNetStudio 8
Право на использование комплекта «Постоянная защита» Средства защиты информации SecretNetStudio LSP
Право на использование Средства защиты информации vGate R2 EnterprisePlus (за 1 физический процессор на защищаемом хосте)
Программный комплекс ViPNetAdministrator 4
Лицензия на 6 месяцев для ПО ViPNetAdministrator 4 (для обучения)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 1-янода) (для образовательных учреждений)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 2-янода) (для образовательных учреждений)
Модуль AdvancedThreatProtection на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль MailSecurity на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль StreamAntivirus на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Лицензия на 1 год для UserGateLogAnalyzer (для образовательных учреждений)
Сенсор для подключения UserGateLogAnalyzer до 5 пользователей (для образовательных учреждений)
Лицензия UserGateManagementCenter на 1 год (для образовательных учреждений)
Сенсор для подключения UserGateManagementCenter до 5 пользователей (для образовательных учреждений)

Учебно-методические пособия:
Учебное пособие по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторная (практическая) работа по курсу UG6P01: Администрирование межсетевых экранов

UserGate 6 (формат pdf)
Материалы слайдов по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторный стенд (программный продукт) по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (в виде образов виртуальных машин)
Учебное пособие: «Безопасность КИИ»
Учебное пособие: «Программно-аппаратный комплекс ViPNetxFirewall»
Учебное пособие: «Технология построения VPN ViPNet. Курс лекций»
Учебное пособие: «Программно-аппаратные комплексы ViPNet HW 4»
Учебное пособие: «Администрирование системы защиты информации ViPNet версии 4»
Учебное пособие «Администрирование ViPNetLinuxCoordinator»
Учебное пособие: «Основы безопасности операционной системы AstraLinuxSpecialEdition. Управление доступом»

Информационное обеспечение реализации программы

1. О. В. Прохорова, Информационная безопасность и защита информации, «Лань», 2021г.;
2. Бубнов А., Пржегорлинский В., Фомина К., Техническая защита информации в объектах информационной инфраструктуры. Учебник. Академия, 2020г.;
3. Скрыль С., Сычев А., Коробец Б., Техническая защита информации: учебник, Академия, 2021г.;
4. С. В. Запечников, О. В. Казарин, А. А. Тарасов, Криптографические методы защиты информации, Академия, 2020г.
5. Сычев Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н.Сычев. — Москва : ИНФРА-М, 2023. — 201 с. — (Среднее профессиональное образование). - ISBN 978-5-16-016583-7. - Текст : электронный. - URL: https://znanium.com/catalog/product/1898839
6. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2024. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст:электронный. - URL: https://znanium.com/catalog/product/2052391

Дополнительные источники:

1. Б.В. Костров, Сети и системы передачи информации, Академия, 2017г.;
2. С.В. Киселев, Основы сетевых технологий, Академия, 2012г.;
3. А.С. Сурядный, Компьютеры, программы, сети, Академия,2015г.

Электронные ресурсы

1. CIT-Forum:Центринформационныхтехнологий:материалысайта[Электронныйресурс]. - Режим доступа: http://citforum.ru/, свободный.
2. Библиотека учебных курсов/ Интернет-Университет информационных технологий - Интуит (Национальный Открытый университет) [Электронный ресурс]. - Режим доступа: http://old.intuit.ru/catalog/, свободный.
3. Материалы Microsoft Virtual Academy [Электронный ресурс]. - Режим доступа: https://www.microsoftvirtualacademy.com/Home.aspx, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения практики и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

При оценивании отчета по практике учитываются оценка уровня прохождения учебной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК3.1.Производить установку, монтаж, настройку и испытания техническихсредств защитыинформации от утечки по техническим каналамв ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные право- вые акты и нормативные методические документы в области за- щиты информации;	**Текущий контроль в форме:** - защитызаданийпоучебной практике; -наблюденияоценкивыполненияработ по учебной практике; -наблюденияпреподавателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференцированныйзачет по учебной практике, производственной практике.
ПК 3.2. Проводить техническое обслу- живание,диагности- ку, устранение не- исправностей и ре- монт технических средств защиты ин- формации, исполь- зуемых в ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные право-	**Текущий контроль в форме:** - защитызаданийпоучебной практике; -наблюденияоценкивыполненияработ по учебной практике; -наблюденияпреподавателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференцированныйзачет по учебной практике, производственной практике.
ПК 3.3. Осуществ- лять защиту инфор- мации от утечки по техническим кана- лам	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров	**Текущий контроль в форме:** - защитызаданийпоучебной практике;

в ИТКС с ис-пользованием тех-нических средств защитывсоответст- вии с предъявляе-мымитребованиями.	электромагнитных излучений и токов, создаваемых техническими средствами защиты ин- формации от утечки по техниче-ским каналам; - применять нормативные право- вые акты и нормативные методические документы в области за- щиты информации;	-наблюденияиоценкив ыполненияработ по учебной практике; -наблюденияпреподав ателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференц ированныйзачет по учебной практике, производственной практике.
ПК3.4.Проводить отдельные работы по физической за- щите линий связи ИТКС.	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в опера ционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно- аппаратных (в том числе крипто- графических) средств защиты информации;	**Текущий контроль в форме:** - защитызаданийпоучебно йпрактике; -наблюденияиоценкив ыполненияработ по учебной практике; -наблюденияпреподав ателязавыполне- нием конкретного задания. **Промежуточный контроль:** комплексныйдифференци рованныйзачет по учебной практике, производственной практике.

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно- программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.4
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности
телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ПРАКТИКИ

профессионального модуля

УП.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи)

СОДЕРЖАНИЕ

2. ПАСПОРТ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ ПО ПРОФЕССИОНАЛЬНЫМ МОДУЛЯМ

Рабочая программа учебной практики является частью основной профессиональной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики является обязательной частью профессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04.

Программа учебной практики определяет содержание и объем знаний, умений, практического опыта которые предстоит приобрести в процессе прохождения практики, а также формирование общих и профессиональных компетенций. В период учебной практики осуществляется:

- практическое обучение студентов профессиональной деятельности;
- формирование умений, практического опыта, общих и профессиональных компетенций по специальности;
- воспитание сознательной трудовой и производственной дисциплины, уважения к трудовым традициям производственного коллектива.

Рабочая программа профессионального модуля может быть использована в дополнительном профессиональном образовании и при повышении квалификации специалистов в области технической эксплуатации телекоммуникационных систем и информационно-коммуникационных сетей связи при наличии среднего общего образования.

Программа учебной практики УП.04 составлена для выполнения части практических занятий с целью освоения практического опыта, умений и знаний по МДК.04.01 Технология выполнения работ по профессии.

Общий объем учебной практики составляет 252 часов.

Рабочая программа разработана для очной формы обучения.

Перечень профессиональных компетенций ПМ.04

Результатом освоения программы производственной практики является овладение обучающимися видом профессиональной деятельности (ВПД): эксплуатация информационно-телекоммуникационных систем и сетей необходимых для последующего освоения ими профессиональных (ПК) и общих (ОК) компетенций:

Код	Наименование видов деятельности профессиональных компетенций
ВД 4.	Выполнение работ по профессии 14601 «Монтажник оборудования связи»
ПК 4.1	Выполнять монтаж, демонтаж и техническое обслуживание кабелей связи и оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами.
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работатьвколлективеикоманде,эффективновзаимодействоватьсколлегами,руководством, клиентами.

ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09.	Использоватьинформационныетехнологиивпрофессиональнойдеятельности.
ОК 10.	Пользоватьсяпрофессиональнойдокументациейнагосударственномииностранном языках.

Цели и планируемые результаты освоения

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе прохождения учебной практики должен:

иметь практический опыт:

- выполнения требований техники безопасности при работе с вычислительной техникой;
- организации рабочего места оператора электронно-вычислительных и вычислительных машин
- инсталляции, настройки и обслуживания программного обеспечения компьютерной системы;
- распечатки, копирования и тиражирования документов на принтере и других устройствах;
- применения офисного программного обеспечения в соответствии с прикладной задачей;
- сканирования документов и их распознавания;
- обработки аудио и визуального контента средствами звуковых, графических и видео-редакторов.

Уметь:

- производить подключение блоков персонального компьютера и периферийных устройств;
- диагностировать простейшие неисправности персонального компьютера, периферийного оборудования и компьютерной оргтехники;
- выполнять инсталляцию системного и прикладного программного обеспечения;
- создавать и управлять содержимым документов с помощью текстовых процессоров;
- создавать и управлять содержимым электронных таблиц с помощью редакторов таблиц;
- создавать и управлять содержимым презентаций с помощью редакторов презентаций;
- создавать и редактировать графические объекты с помощью программ для обработки растровой графики;
- редактировать звук в звуковом редакторе.

Знать:

- требования техники безопасности при работе с вычислительной техникой;
- основные принципы устройства и работы компьютерных систем и периферийных устройств;
- виды носителей информации;
- назначение, разновидности и функциональные возможности текстовых редакторов;
- назначение, разновидности и функциональные возможности табличных процессоров;
- назначение, разновидности и функциональные возможности программ обработки звука;
- назначение, разновидности и функциональные возможности графических редакторов;
- назначение, разновидности и функциональные возможности редакторов презентаций.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

Наименование разделовитем профессиональ ного модуля (ПМ), междисциплин арных курсов (МДК)	**Содержаниеучебногоматериала,лабораторныеработыи практическиезанятия,внеаудиторная(самостоятельная) учебная работа обучающихся, курсовая работа (проект)**	**Объ ем часо в**	**Уро вень осво ения**
1	**2**	**3**	
Раздел 1.Владение технологией монтажа медно-жильных и волоконно-оптическихкабельныхлинийсвязи,структурированныхкабельныхсистем			
Технологиямонтажакабелейсвязи		**36**	
Тема1. Виды кабелей связи и их назначение	**Содержание**	**20**	
	Медно-жильныекабели связи. Виды кабелей связи для городских и сельских сетейсвязиих назначение.	20	3
	Волоконно-оптические кабели связи. Виды кабелей связи для городских и сельскихсетейсвязи.Их назначение.		3
Тема2. Материалы и инструменты для монтажа кабелейсвязи	**Содержание**	**28**	
	Материалыиинструментыдлямонтажамедно-жильныхкабелей связи. Виды материалов для монтажа. Их назначение. Инструменты для монтажа. Ихназначение.	28	3
	Материалы и инструменты для монтажа волоконно- оптических кабелей связи.		3
Тема3.	**Содержание**	**76**	

Прядок проведения работ по монтажу кабелейсвязи	Порядокпроведенияработпомонтажукабелей связи. Технология монтажа медно-жильных кабелей связи. Разделка кабеля. Подготовка кабеля для монтажа. Технология монтажа волоконно-оптических кабелей связи	10	3
	Практическоезанятие	**30**	
	Осуществлениеэтаповподготовкикабелядлямонтажа	**6**	3
	Изготовлениешнуровзаземлениядля телекоммуникационного оборудования	**6**	
	Подключение волоконно-оптического кабеля к	**6**	
	телекоммуникационномуоборудованию		
	Осуществление выбора материала и инструментов для монтажакабелейсвязи	**4**	
	Осуществлениевыборакабелясвязидля монтажа.	**4**	
Тема4. Технология подсоединения волоконно-оптического кабеля к телекоммуника ционному оборудованию	**Содержание**	**4**	
	Подсоединение волоконно-оптического кабеля к телекоммуникационномуоборудованию.	10	3
	Монтаж телекоммуникационных шкафов. Особенности монтажа. Технология запайки муфт. Монтаж стоек 19”. Технологическая последовательность пайки.		3
Тема5. Обеспечение техники безопасности при монтаже и эксплуатации телекоммуника ционного оборудования	**Содержание**	**6**	
	Обеспечение техники безопасности при монтаже и эксплуатации телекоммуникационного оборудования	6	3
Учебная практика Виды работ:	**Содержание** Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получениезаданияпотематике.Правилаоформленияотчетов и презентации.	2	2

	Монтажкабельныхизделийвсоответствиисмаркировкойи назначением	2	3
	Осуществление монтажа коммутационных шнуров с использованием различных видов арматуры методом обжимки.	16	3
	Осуществлениемонтажакоммутационныхшнуровметодом накрутки.	16	3
	Монтажоптическихкабелейвсоответствиисконструкциейи назначением.	16	3
	Осуществлениеразделкиоптическогокабеля	12	3
	Монтажподвескиоптическогокабелякопорамздания.	16	3
	Монтажподвескиоптическогокабелякопорамэлектрических сетей.	16	3
	Выполнение оконцовки оптического кабеля. Сварка оптическихволокон.	12	3
	Осуществление проверки качества сварки оптических волокон,волоконно-оптическихкабелей.	12	3
	Изучениеконструкцийиназначенияоптических муфт.	4	2
	Выполнение технологической последовательности пайки оптических муфт, дефекты, методы предупреждения и способыустраниядефектов.	16	3
	Выполнениегерметизациимуфтпотехнологии3М.	12	3
	Подготовкаконструкцииоптическихкроссовкмонтажу.	14	3
	Выполнениетехнологическойпоследовательностимонтажа оптическогокроссанастенноговарианта.	16	3
	Выполнениетехнологическойпоследовательностимонтажа	16	3
	оптическогокроссастоечноговарианта.		
	Выполнениевводакабелявоптическийкросснастенного вариантаистоечного варианта.	12	3
Итого по учебной практике:	**252**		

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Учебная практика профессионального модуля ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих по профилю специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем проходит «лаборатория технических средств информатизации. Программных и программно – аппаратных средств защиты информации», оснащенная необходимым для реализации программы практики оборудованием.

Оборудование кабинета: рабочее место преподавателя; рабочие места обучающихся, доска аудиторная, мультимедийное оборудование, системный блок, монитор.

Программное обеспечение:

Простая (неисключительная) лицензия на Программное обеспечение «Рубикон» - комплекс межсетевого экранирования и средство обнаружения вторжений
Простая (неисключительная) лицензия на Программное обеспечение «Сканер-ВС»
Простая (неисключительная) лицензия на Программное обеспечение «Программное обеспечение KOMRAD Enterprise SIEM»
Неискл. право DallasLock 8.0-K (СЗИ НСД, СКН, МЭ, СОВ, МП, РК, СКН2) (для обучения)
Неискл. право DallasLock ЕЦУ 3 устройства (для обучения)
Неискл. право DallasLockLinux (СЗИ НСД, СКН) (для обучения)
Несертифицированный комплект для установки DallasLock 8.0-K (для обучения)
Несертифицированный комплект для установки DallasLockLinux (для обучения)
Право на использование модулей защиты от НСД и контроля устройств средства защиты информации SecretNetStudio 8
Право на использование модулей защиты диска и шифрования контейнеров средства защиты информации SecretNetStudio 8
Право на использование модуля персонального межсетевого экрана средства защиты информацииSecretNetStudio 8
Право на использование комплекта «Постоянная защита» Средства защиты информации SecretNetStudio LSP
Право на использование Средства защиты информации vGate R2 EnterprisePlus (за 1 физический процессор на защищаемом хосте)
Программный комплекс ViPNetAdministrator 4
Лицензия на 6 месяцев для ПО ViPNetAdministrator 4 (для обучения)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 1-янода) (для образовательных учреждений)
Лицензия для UserGate на 1 год до 5 пользователей (кластер, 2-янода) (для образовательных учреждений)
Модуль AdvancedThreatProtection на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль MailSecurity на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Модуль StreamAntivirus на 1 год для UserGate до 5 пользователей (для образовательных учреждений)
Лицензия на 1 год для UserGateLogAnalyzer (для образовательных учреждений)
Сенсор для подключения UserGateLogAnalyzer до 5 пользователей (для образовательных учреждений)
Лицензия UserGateManagementCenter на 1 год (для образовательных учреждений)
Сенсор для подключения UserGateManagementCenter до 5 пользователей (для образовательных учреждений)

Учебно-методические пособия:
Учебное пособие по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)

Лабораторная (практическая) работа по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Материалы слайдов по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (формат pdf)
Лабораторный стенд (программный продукт) по курсу UG6P01: Администрирование межсетевых экранов UserGate 6 (в виде образов виртуальных машин)
Учебное пособие: «Безопасность КИИ»
Учебное пособие: «Программно-аппаратный комплекс ViPNetxFirewall»
Учебное пособие: «Технология построения VPN ViPNet. Курс лекций»
Учебное пособие: «Программно-аппаратные комплексы ViPNet HW 4»
Учебное пособие: «Администрирование системы защиты информации ViPNet версии 4»
Учебное пособие «Администрирование ViPNetLinuxCoordinator»
Учебное пособие: «Основы безопасности операционной системы AstraLinuxSpecialEdition. Управление доступом»

Информационное обеспечение реализации программы

1. Линиисвязинажелезнодорожномтранспорте:учебник/А.К.Канаев,В.А. Кудряшов, А.К. Тощев . – Москва : ФГБУ ДПО «УМЦ ЖДТ», 2017. – 412 с.Режим доступа: http://umczdt.ru/books/44/62162/— ЭБ «УМЦ ЖДТ»
2. Нефедов,В.И.Теорияэлектросвязи :учебникдляСПО/В. И.Нефедов, А.С.Сигов;подредакциейВ. И.Нефедова. —Москва:ИздательствоЮрайт, 2020. — 495 с. ЭБС Юрайт [сайт]. — URL: http://www.biblio-online.ru/bcode/451173
3. Сажнев,А.М. Электропреобразовательныеустройстварадиоэлектронных средств:учебное пособие длявузов /А.М. Сажнев, Л.Г.Рогулина.—2-е изд., испр. и доп.— Москва: ИздательствоЮрайт,2020. — 204с.ЭБС Юрайт [сайт]. — URL: http://biblio-online.ru/bcode/446283
4. Романюк,В.А. Основырадиосвязи :учебникдлявузов /В.А.Романюк.— Москва:ИздательствоЮрайт,2020. —288с.ЭБСЮрайт[сайт].— URL: http://www.biblio-online.ru/bcode/449710
5. Гагарина,Л. Г. Технические средства информатизации: учебное пособие / Л.Г. Гагарина, Ф.С.Золотухин. — 2-е изд., перераб. и доп. — Москва: ИНФРА-М, 2021. — 260 с. — (Среднее профессиональное образование).

Электронные ресурсы

1. CIT-Forum:Центринформационныхтехнологий:материалысайта[Электронныйресурс]. - Режим доступа: http://citforum.ru/, свободный.
2. Библиотека учебных курсов/ Интернет-Университет информационных технологий - Интуит (Национальный Открытый университет) [Электронный ресурс]. - Режим доступа: http://old.intuit.ru/catalog/, свободный.
3. Материалы Microsoft Virtual Academy [Электронный ресурс]. - Режим доступа: https://www.microsoftvirtualacademy.com/Home.aspx, свободный.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения практики и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

При оценивании отчета по практике учитываются оценка уровня прохождения учебной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Код и наименование профессиональных компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1 Выполнять монтаж, демонтаж и техническое обслуживание кабелей связии оконечных структурированных кабельных устройств в соответствии с действующими отраслевыми стандартами	- выбор марки и типа кабеля осуществляется в соответствии с проектом и исходя из условий прокладки структурированных кабельных систем сетей широкополосного доступа в соответствии с действующими отраслевыми стандартами; - коммутация сетевого оборудованияи рабочих станций заданнойтопологи производится в соответствии с действующими отраслевыми стандартами; - техническая документацияи формы(формуляры, паспорта, оперативные журналыит.п.) заполняются в соответствии с действующими отраслевыми стандартами	**Текущий контроль в форме:** - защиты заданий по учебной практике; - наблюдения и оценки выполнения работ по учебной практике; - наблюдения преподавателя за выполнением конкретного задания. **Промежуточный контроль в форме:** комплексныйдифференцированныйзачет по учебной практике, производственной практике.

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материала, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.5
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности телекоммуникационных
систем

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПОПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по профессиональным модулям ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей.

Область применения программы

Программа производственной практики по ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части приобретения практического опыта в процессе освоения основного вида профессиональной деятельности (ВД): Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 1.	Эксплуатацияинформационно-телекоммуникационныхсистемисетей
ПК 1.1.	Производить монтаж, настройку, проверку функционирования и конфигурированиеоборудованияинформационно-телекоммуникационных системисетей.
ПК 1.2.	Осуществлятьдиагностикутехническогосостояния,поискнеисправностейи ремонтоборудованияинформационно-телекоммуникационныхсистемисетей.
ПК 1.3.	Проводитьтехническоеобслуживаниеоборудованияинформационно - телекоммуникационныхсистемисетей.
ПК 1.4.	Осуществлятьконтрольфункционированияинформационно-телекоммуникационныхсистемисетей.

Цели и задачи практики

Производственная практика в виде практической подготовки направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ПООП (примерные основные образовательные программы) СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем: квалификация - техник по защите информации

Производственная практика базируется на междисциплинарных курсах профессионального модуля:

• МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания;

• МДК.01.02.Телекоммуникационные системы и сети

• МДК.01.03.Электрорадиоизмерения и метрология

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций в результате прохождения практической подготовки обучающийся должен:

Иметь практический опыт в	монтаже,настройке,проверкефункционированияи конфигурировании оборудования ИТКС; текущемконтролефункционированияоборудования ИТКС; проведениитехническогообслуживания,диагностикетехнического состояния, поиске неисправностей и ремонте оборудования ИТКС.

уметь	осуществлятьтехническуюэксплуатациюлинейныхсооружений связи; производитьмонтажкабельныхлинийиоконечныхкабельных устройств; настраивать,эксплуатироватьиобслуживатьоборудование ИТКС; осуществлятьподключение,настройкумобильныхустройстви распределенных сервисов ИТКС; производитьиспытания,проверкуиприемкуоборудования ИТКС; проводитьработыпотехническомуобслуживанию,диагностике технического состояния и ремонту оборудования ИТКС.
знать	принципыпостроенияиосновныххарактеристикинформационно-телекоммуникационных систем и сетей (далее - ИТКС); принципыпередачиинформациивИТКС; виды ихарактеристикисигналов в ИТКС; видыпомех вканалах связиИТКСиметодызащитыотних; разновидностилинийпередач,конструкцииихарактеристики электрических и оптических кабелей связи; технологииоборудованиеудаленногодоступавИТКС; принципыпостроения,основныехарактеристикиактивногосетевогои коммуникационного оборудования ИТКС.

Количество часов на освоение программы производственной практики (по профилю специальности)

ПП.01. Эксплуатация информационно-телекоммуникационных систем и сетей:
производственная практика(по профилю специальности)по ПМ.01. –108 часов,втом числе в форме практической подготовки – 108 часов.
Форма промежуточной аттестации–дифференцированный зачет.

Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.01. Эксплуатация информационно-телекоммуникационных систем и сетей является овладение профессиональными (ПК) и общими (ОК)компетенциями:

Код компетенции	**Наименованиерезультатаобучения**
ВД1.	Защитаинформациивинформационно-телекоммуникационныхсистемахи сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
ПК 1.1.	Производить монтаж, настройку, проверку функционирования и конфигурированиеоборудованияинформационно-телекоммуникационных системисетей.
ПК 1.2.	Осуществлятьдиагностикутехническогосостояния,поискнеисправностейи ремонтоборудованияинформационно-телекоммуникационныхсистеми сетей.
ПК 1.3.	Проводитьтехническоеобслуживаниеоборудованияинформационно - телекоммуникационныхсистемисетей.

ПК 1.4.	Осуществлятьконтрольфункционированияинформационно-телекоммуникационныхсистемисетей.
ОК 01	Выбиратьспособырешениязадачпрофессиональнойдеятельности, применительнокразличнымконтекстам
ОК 02	Осуществлятьпоиск,анализиинтерпретациюинформации,необходимой длявыполнениязадачпрофессиональнойдеятельности
ОК 03	Планироватьиреализовыватьсобственноепрофессиональноеиличностное развитие
ОК 04	Работатьвколлективеикоманде,эффективновзаимодействоватьс коллегами,руководством,клиентами
ОК 09	Использоватьинформационныетехнологиивпрофессиональной деятельности
ОК 10	Пользоватьсяпрофессиональнойдокументациейнагосударственноми иностранномязыках

2. СТРУКТУРАИСОДЕРЖАНИЕПРОИЗВОДСТВЕННОЙПРАКТИКИ(ПОПРОФИЛЮСПЕЦИАЛЬНОСТИ)

Код профессиональных компетенций	**Наименования профессионального модуля, МДК**	**Количество часов на производственную практику, по соответствующему МДК**	**Виды работ**
ПМ.01.ЭКСПЛУАТАЦИЯИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХСИСТЕМИСЕТЕЙ			
	МДК.01.01. Приемо-передающиеустройства, линейные сооружения связи и источники электропитания	10	Монтажкабельныхлинийиоконечныхкабельныхустройств
			ИТКС;
ПК 1.1.		10	Проверкафункционирования,выполнениерегулировкии
ПК 1.2.			контролюосновныхпараметровисточниковпитанияИТКС;
ПК 1.3. ПК 1.4.		10	Осуществлениетехническойэксплуатациилинейных сооружений связи;
		10	Осуществлениетехническойэксплуатациилинейных
			сооружений ИТКС.
			Измерениеосновныхпоказателейихарактеристикапри
		8	выполненииработпонастройке,проверкефункционирования
			иконфигурированияИТКС;
			Измерениеосновныхпараметровихарактеристикпри
ПК 1.1. ПК 1.2. ПК 1.3. ПК 1.4.	МДК.01.02. Телекоммуникационные системы и сети	8	выполненииработподиагностикетехническогосостояния, поиска неисправностей и ремонте оборудования ИТКС;
		8	Измерениеосновныхпараметровихарактеристикпри выполнениитехническогообслуживанияоборудования ИТКС
		6	Мониторингиконтрольфункционированияоборудования
			ИТКС;
		8	Измерениеосновныхпараметровихарактеристик
			оборудованияИТКС;
		6	Ведениеэксплуатационно-технической документациина оборудованиеИТКС.
ПК 1.1.	МДК.01.03.	12	Проверкафункционированияосновныхпараметров источников питания радиоаппаратуры

ПК 1.2. ПК 1.3. ПК 1.4.	Электрорадио измерения и метрология	12	Регулировкаиконтрольосновныхпараметровисточников питания радиоаппаратуры
ВСЕГО часов	**108**		

3. УСЛОВИЯРЕАЛИЗАЦИИПРОГРАММЫ ПРОИЗВОДСТВЕННОЙПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся:

ООО «ФАБРИКА «ДОНБАСС-ЛИБЕРТИ»

Реализация рабочей программы производственной практики предусмотрены следующие специальные помещения: участок металлической мебели мебельного производства.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

ФИЛИАЛ № 1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВАОД «СИЛУР» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РОСТЭКСПОСНАБ 8»

Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

Информационное обеспечение реализации программы

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУМИРЭА,2021.—79с.—Текст :электронный //Лань:электронно- библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5- 4488-0070-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995 (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей

3. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ(МИИТ),2019.—144с.—ISBN978-5-7876-0326-2.—Текст:электронный//
Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей

Общие требования к организации практики

К прохождению производственной практики допускаются обучающиеся, не имеющие академической задолженности по междисциплинарным курсам и учебным практикам в рамках освоения профессионального модуля ПМ.01.Эксплуатация информационно-телекоммуникационных систем и сетей по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Организация производственной практики осуществляется в сроки, установленные рабочим учебным планом, после изучения всего раздела междисциплинарного курса или чередуясь с темами теоретического обучения.

Максимальный объем производственной практики составляет 36 академических часов в неделю.

База практики должна соответствовать профилю специальности обучающегося.

На предприятии за студентом закрепляется руководитель, который проводит с ним инструктаж по технике безопасности, охране труда, знакомит обучающегося со структурой предприятия, помогает освоить темы производственной практики и осуществляет контроль ее прохождения. В колледже подготовкой обучающегося к производственной практике, консультацией по вопросам прохождения практики занимается заведующий практикой.

Во время прохождения практики обучающийся ведет дневник практики, в котором руководитель от предприятия делает отметки и выставляет оценки. В конце практики студент оформляет отчет по производственной практике, согласно требованиям по составлению технического отчета. Руководитель практики от предприятия дает отзыв- характеристику о сформировавшихся у практиканта общих и профессиональных компетенциях, что учитывается в дальнейшем при получении итоговой оценки по практике.

Аттестация по итогам производственной практики (по профилю специальности) проводится с учетом результатов ее прохождения, подтверждаемых документами соответствующих организаций (баз практик). Студент должен представить в колледж для получения оценки по практике: технический отчет с выполненным заданием, заполненный дневник, аттестационный лист, который выдается студентам в колледже.

4. КОНТРОЛЬИОЦЕНКАРЕЗУЛЬТАТОВОСВОЕНИЯПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Одной из форм контроля результатов производственной практики является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

При оценивании отчета по практике учитываются оценка уровня прохождения производственной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Аттестация по итогам производственной практики – дифференцированный зачет - проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК1.1.Производитьмонтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверятьфункционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерятьосновные показателиихарактеристики при выполнении работ по настройке, проверке функционирования и конфигурированияИТКС;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания
ПК 1.2. Осуществлять диагностикутехнического состояния, поиск неисправностейиремонт оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений связи; - проверятьфункционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; - измерятьосновныепараметры и характеристики при выполнении работ по диагностикетехнического состояния, поиска неисправностейиремонте оборудования ИТКС;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания

ПК 1.3**.** Проводить техническоеобслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений ИТКС; - измерятьосновные параметры и характеристики привыполнениитехнического обслуживания оборудования ИТКС; производитьконтрольи регулировку основных параметров источников питанияоборудованияИТКС;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания
ПК1.4**.** Осуществлять контрольфункционирования ИТКС	-проводитьмониторинги контрольфункционирования оборудованияИТКС; -измерять основные параметрыи характеристики оборудованияИТКС; -вестиэксплуатационно-техническуюдокументациюна оборудованиеИТКС;	-наблюдениеза действиямина практике -оценкадействийна практике -оценка результатов дифференцированного зачета Дневникпрактики, Аттестационныйлист, описательнаячасть техническогоотчетапо выполнению индивидуальногозадания

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.6
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности телекоммуникационных
систем

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по профессиональным модулям ПМ.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты.

Область применения программы

Программа производственной практики по ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты, является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части приобретения практического опыта в процессе освоения основного вида профессиональной деятельности (ВД): Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименованиевидовдеятельностиипрофессиональныхкомпетенций**
ВД 2.	Защитаинформациивинформационно-телекоммуникационныхсистемахисетях с использованием программных и программно-аппаратных, в том числе Криптографических средств защиты
ПК 2.1	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.
ПК 2.2	Поддерживатьбесперебойнуюработупрограммныхипрограммно-аппаратных,в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальныхвоздействийвинформационно-телекоммуникационныхсистемахи сетях с использованием программных и программно-аппаратных, в том числе криптографическихсредстввсоответствииспредъявляемымитребованиями.

Цели и задачи практики

Производственная практика в виде практической подготовки направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ПООП (примерные основные образовательные программы) СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем: квалификация - техник по защите информации

Производственная практика базируется на междисциплинарных курсах профессионального модуля:

• МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты;

• МДК.02.02.Криптографическая защита информации.

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций в результате прохождения практической подготовки обучающийся должен:

Иметь практический опыт в	установке, настройке, испытаниях и конфигурировании программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей; поддержании бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях; защите информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных, втом числе криптографических средств защиты в соответствии с предъявляемыми требованиями.
уметь	выявлять и оценивать угрозы безопасности информации в ИТКС; настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить установку и настройку программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить контроль показателей и процесса функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить восстановление процесса и параметров функционирования программных и программно-аппаратных, в том числе криптографических средств защиты информации; проводить техническое обслуживание и ремонт программно-аппаратных, в том числе криптографических средств защиты информации.
знать	возможные угрозы безопасности информации в ИТКС; способы защиты информации от несанкционированного доступа (далее - НСД) и специальных воздействий на нее; типовые программные и программно-аппаратные средства защиты информации в информационно-телекоммуникационных системах и сетях; криптографические средства защиты информации конфиденциального характера, которые применяются в информационно-телекоммуникационных системах и сетях; порядок тестирования функций программных и программно-аппаратных, в том числе криптографических средств защиты информации; организацию и содержание технического обслуживания и ремонта программно-аппаратных, в том числе криптографических средств защиты информации; порядок и правила ведения эксплуатационной документации на программные и программно-аппаратные, в том числе криптографические средства защиты информации.

Количество часов на освоение программы производственной практики (по профилю специальности)

ПП.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты:
производственная практика(по профилю специальности)по ПМ.02. –112 часов.
Форма промежуточной аттестации–дифференцированный зачет.

Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты является овладение профессиональными (ПК) и общими (ОК) компетенциями:

Код компетенции	**Наименованиерезультатаобучения**
ВД 2.	Защитаинформациивинформационно-телекоммуникационныхсистемахисетях с использованием программных и программно-аппаратных, в том числе криптографическихсредствзащиты
ПК 2.1	Производитьустановку,настройку,испытанияиконфигурированиепрограммных и программно-аппаратных, в том числе криптографических средств защиты информацииотнесанкционированногодоступаиспециальныхвоздействийв оборудованиеинформационно-телекоммуникационныхсистемисетей.
ПК 2.2	Поддерживатьбесперебойнуюработупрограммныхипрограммно-аппаратных,в том числе криптографических средств защиты информации в информационно- телекоммуникационных системах и сетях.
ПК 2.3	Осуществлять защиту информации от несанкционированных действий и специальныхвоздействийвинформационно-телекоммуникационныхсистемахи сетях с использованием программных и программно-аппаратных, в том числе криптографическихсредстввсоответствииспредъявляемымитребованиями.
ОК 01	Выбиратьспособырешениязадачпрофессиональнойдеятельности, применительнокразличнымконтекстам
ОК 02	Осуществлятьпоиск,анализиинтерпретациюинформации,необходимой длявыполнениязадачпрофессиональнойдеятельности
ОК 03	Планироватьиреализовыватьсобственноепрофессиональноеиличностное развитие
ОК 04	Работатьвколлективеикоманде,эффективновзаимодействоватьс коллегами,руководством,клиентами
ОК 09	Использоватьинформационныетехнологиивпрофессиональной деятельности
ОК 10	Пользоватьсяпрофессиональнойдокументациейнагосударственноми иностранномязыках

2. СТРУКТУРАИСОДЕРЖАНИЕПРОИЗВОДСТВЕННОЙПРАКТИКИ(ПОПРОФИЛЮСПЕЦИАЛЬНОСТИ)

Код профессиональных компетенций	**Наименования профессионального модуля, МДК**	**Количество часов на производственную практикупоПМ.03,по соответствующему МДК**	**Виды работ**
ПМ.02.Защитаинформациивинформационно-телекоммуникационныхсистемахисетяхсиспользованиемпрограммныхи программно-аппаратных,втомчислекриптографических,средствзащиты			
ПК 2.1 ПК 2.2 ПК 2.3	МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных ипрограммно-аппаратных средств защиты.	10	Участиеворганизацииработпозащите персональных компьютеровнапредприятии
		8	Участиеворганизацииработпозащителокальныхсетейна предприятии
		8	Участиеворганизацииработпозащитеработв глобальной сетиинтернетна предприятии
		8	Ознакомление,организация,настройкасистембезопасности проводнойзащищеннойлокальнойсети
		8	Администрированиесистембезопасностипроводной защищеннойлокальнойсети
		8	Ознакомление,организация,настройкасистембезопасности
			беспроводнойзащищеннойлокальнойсети
ПК 2.1 ПК 2.2 ПК 2.3	МДК.02.02. Криптографическая защитаинформации.	8	Администрированиесистембезопасностибеспроводной защищеннойлокальнойсети
			Поддержаниебесперебойнойработыпрограммныхи
		8	программно-аппаратных,втомчислекриптографических средствзащитыинформациив оборудовании
			информационно-телекоммуникационныхсистемисетей
		6	Выборпрограммныхсредствшифрованиявсоответствиис решаемой задачей
		8	Подключение,установкадрайверов,настройкапрограммных средств абонентского шифрования

		6	Администрированиевнедренныхсредств
		8	Настройкасредствэлектроннойподписи
		6	Администрированиесредствэлектроннойподписи
		6	АдминистрированиесредствPKI
		6	Сдачатехническогоотчета,получениеоценкиКДЗ
ВСЕГО часов		**112**	

3. УСЛОВИЯРЕАЛИЗАЦИИПРОГРАММЫ ПРОИЗВОДСТВЕННОЙПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся:

ООО «ФАБРИКА «ДОНБАСС-ЛИБЕРТИ»

Реализация рабочей программы производственной практики предусмотрены следующие специальные помещения: участок металлической мебели мебельного производства.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

ФИЛИАЛ № 1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВАОД «СИЛУР» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РОСТЭКСПОСНАБ 8»

Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

Информационное обеспечение реализации программы

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУМИРЭА,2021.—79с.—Текст :электронный //Лань:электронно- библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5- 4488-0070-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995 (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей

3. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ(МИИТ),2019.—144с.—ISBN978-5-7876-0326-2.—Текст:электронный//

Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей

Общие требования к организации практики

К прохождению производственной практики допускаются обучающиеся, не имеющие академической задолженности по междисциплинарным курсам и учебным практикам в рамках освоения профессионального модуля ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Организация производственной практики осуществляется в сроки, установленные рабочим учебным планом, после изучения всего раздела междисциплинарного курса или чередуясь с темами теоретического обучения.

Максимальный объем производственной практики составляет 36 академических часов в неделю.

База практики должна соответствовать профилю специальности обучающегося.

На предприятии за студентом закрепляется руководитель, который проводит с ним инструктаж по технике безопасности, охране труда, знакомит обучающегося со структурой предприятия, помогает освоить темы производственной практики и осуществляет контроль ее прохождения. В колледже подготовкой обучающегося к производственной практике, консультацией по вопросам прохождения практики занимается заведующий практикой.

Во время прохождения практики обучающийся ведет дневник практики, в котором руководитель от предприятия делает отметки и выставляет оценки. В конце практикистудентоформляет отчет по производственной практике, согласно требованиям по составлению технического отчета. Руководитель практики от предприятия дает отзыв- характеристику о сформировавшихся у практиканта общих и профессиональных компетенциях, что учитывается в дальнейшем при получении итоговой оценки по практике.

Аттестация по итогам производственной практики (по профилю специальности) проводится с учетом результатов ее прохождения, подтверждаемых документами соответствующих организаций (баз практик). Студент должен представить в колледж для получения оценки по практике: технический отчет с выполненным заданием, заполненный дневник, аттестационный лист, который выдается студентам в колледже.

4. КОНТРОЛЬИОЦЕНКАРЕЗУЛЬТАТОВОСВОЕНИЯПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Одной из форм контроля результатов производственной практики является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

При оценивании отчета по практике учитываются оценка уровня прохождения производственной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Аттестация по итогам производственной практики – дифференцированный зачет - проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 2.1. Производить установку,настройку, испытания и конфигурирование программныхипрограммно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступаи специальных воздействийоборудование информационно-телекоммуникационных систем и сетей.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средствазащитыинформациив операционных системах, в том числе средства антивирусной защиты; - проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания
ПК 2.2. Поддерживать бесперебойную работу программных ипрограммно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации; - проводить техническое обслуживание и ремонт	- наблюдение за действиямина практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

	программно-аппаратных (в том числе криптографических) средств защиты информации;	
ПК 2.3.Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных ипрограммно-аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	-выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.7
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности телекоммуникационных
систем

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по профессиональным модулям ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты.

Область применения программы

Программа производственной практики по ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты, является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части приобретения практического опыта в процессе освоения основного вида профессиональной деятельности (ВД): Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименованиевидовдеятельностиипрофессиональныхкомпетенций**
ВД 3.	Защитаинформациивинформационно-телекоммуникационныхсистемахисетях с использованием технических средств защиты
ПК 3.1	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием техническихсредствзащитывсоответствииспредъявляемымитребованиями.
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационных систем и сетей.

Цели и задачи практики

Производственная практика в виде практической подготовки направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ПООП (примерные основные образовательные программы) СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем: квалификация - техник по защите информации

Производственная практика базируется на междисциплинарных курсах профессионального модуля:

• МДК.03.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты;

• МДК.03.02. Физическая защита линий связи информационно-телекоммуникационных систем и сетей.

• МДК.03.03. Технология выполнения работ по одной или нескольким профессиям рабочих, должностям служащих;

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций в результате прохождения практической подготовки обучающийся должен:

Иметь практический опыт в	выявление технических каналов утечки информации; защита информации от утечки по техническим каналам с использованием техническихсредствзащитывсоответствииспредъявляемымитребованиями; проведение измерений параметров фоновых шумов, а так же физических полей, создаваемых техническими средствами защиты информации; проведение технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам; установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам;.
уметь	применять нормативные правовые акты инормативные методические документы в области защиты информации; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; проводитьизмерениепараметровфоновыхшумовипобочныхэлектромагнитных излучений и наводок (далее - ПЭМИН), создаваемых оборудованием ИТКС; проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защитыинформации от утечки по техническим каналам; проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; использовать средства физической защиты линий связи ИТКС;
знать	способызащитыинформацииотутечкипотехническимканаламсиспользованием технических средств защиты; номенклатурупримен яемыхсредствзащитыинформациионесанкционированной утечки по техническим каналам; основныетипытехническихсредствзащитыинформациииотутечкипо техническим каналам; методики измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации от утечки по техническим каналам; организациюисодержаниетехническогообслуживанияиремонтатехнических средств защиты информации от утечки по техническим каналам; порядокиправилаведенияэксплуатационнойдокументациинатехнические средства защиты информации от утечки по техническим каналам; содержаниеиорганизациюработпофизическойзащителинийсвязиИТКС; принципыдействияиосновныехарактеристикитехническихсредствфизической защиты; законодательствообластиинформационнойбезопасности,структуру государственнойсистемызащитыинформации,нормативныхправовыхактовуполномоченныхоргановвисполнительнойвласти,национальныхстандартовидругих методических документов в области информационной безопасности; принципыиметодыорганизационнойзащитыинформации,организационного обеспечения информационной безопасности в организациях

Количество часов на освоение программы производственной практики (по профилю специальности)

ПП.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты:
производственная практика (по профилю специальности)по ПМ.03. –108 часов.
Форма промежуточной аттестации–дифференцированный зачет.

Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты является овладение профессиональными (ПК) и общими (ОК) компетенциями:

Код компетенции	**Наименованиерезультатаобучения**
ПК 3.1	Производитьустановку,монтаж,настройкуииспытаниятехническихсредств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.
ПК 3.2	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемыхвинформационно-телекоммуникационныхсистемахисетях.
ПК 3.3	Осуществлять защиту информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях с использованием техническихсредствзащитывсоответствииспредъявляемыми требованиями.
ПК 3.4	Проводить отдельные работы по физической защите линий связи информационно-телекоммуникационныхсистемисетей.
ОК 01	Выбиратьспособырешениязадачпрофессиональнойдеятельности, применительнокразличнымконтекстам
ОК 02	Осуществлятьпоиск,анализиинтерпретациюинформации,необходимой длявыполнениязадачпрофессиональнойдеятельности
ОК 03	Планироватьиреализовыватьсобственноепрофессиональноеиличностное развитие
ОК 04	Работатьвколлективеикоманде,эффективновзаимодействоватьс коллегами,руководством,клиентами
ОК 05	Осуществлятьустнуюиписьменнуюкоммуникациюнагосударственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлятьгражданско-патриотическуюпозицию,демонстрировать осознанноеповедениенаосноветрадиционныхобщечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействоватьсохранениюокружающейсреды,ресурсосбережению, эффективнодействоватьвчрезвычайныхситуациях.
ОК 09	Использоватьинформационныетехнологиивпрофессиональной деятельности

2. СТРУКТУРАИСОДЕРЖАНИЕПРОИЗВОДСТВЕННОЙПРАКТИКИ(ПОПРОФИЛЮСПЕЦИАЛЬНОСТИ)

Код профессиональных компетенций	**Наименования профессионального модуля, МДК**	**Количество часов на производственную практикупоПМ.03,по соответствующему МДК**	**Виды работ**
ПМ.03.Защитаинформациивинформационно-телекоммуникационныхсистемахисетяхсиспользованиемтехническихсредств защиты			
ПК 3.1 – ПК 3.4 ОК 01-ОК 07, ОК 09	МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием техническихсредствзащиты	6	Участиевмонтажетехническихсредствзащиты информации;
		6	Участиевобслуживаниитехническихсредствзащиты информации;
		6	Участиевэксплуатациитехническихсредствзащиты информации;
		6	Участиевмонтажесредствохраныибезопасности, инженернойзащитыитехническойохраныобъектов;
		6	Участиевобслуживании средствохраныи безопасности, инженернойзащитыитехническойохраныобъектов;
		6	Участиевэксплуатациисредствохраныи безопасности, инженернойзащитыитехническойохраныобъектов;
		6	Участиевмонтажесистемвидеонаблюдения;
		6	Участиевобслуживаниисистемвидеонаблюдения;
		6	Участиевэксплуатациисистемвидеонаблюдения;
		14	Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.
ПК 3.1 – ПК 3.4	МДК.03.02.Физическая защита линий связи	10	Участие в монтаже средств защиты информации от несанкционированногосъѐма;
		10	Участие в монтаже средств защиты информации от утечки по техническим каналам;
		10	Участиевобслуживаниисредствзащитыинформации утечки потехническимканалам;

ОК 01-ОК 07, ОК 09	информационно-телекоммуникационных систем и сетей	10	Участиевэксплуатациисредствзащитыинформации утечки потехническимканалам
ВСЕГО часов		**108**	

3. УСЛОВИЯРЕАЛИЗАЦИИПРОГРАММЫ ПРОИЗВОДСТВЕННОЙПРАКТИКИ

Требования к минимальному материально-техническому обеспечению

Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся:

ООО «ФАБРИКА «ДОНБАСС-ЛИБЕРТИ»

Реализация рабочей программы производственной практики предусмотрены следующие специальные помещения: участок металлической мебели мебельного производства.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

ФИЛИАЛ № 1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВАОД «СИЛУР» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РОСТЭКСПОСНАБ 8»

Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта.

Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.

Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.

Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.

Локальная сеть с выходом в Интернет.

Информационное обеспечение реализации программы

1. Леонтьев, А. С. Защита информации : учебное пособие / А. С. Леонтьев. — Москва : РТУМИРЭА,2021.—79с.—Текст :электронный //Лань:электронно- библиотечная система. — URL: https://e.lanbook.com/book/182491 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5- 4488-0070-2. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/87995 (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей

3. Груздева, Л. М. Защита информации : учебное пособие / Л. М. Груздева. — Москва : РУТ(МИИТ),2019.—144с.—ISBN978-5-7876-0326-2.—Текст:электронный//

Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/188703 (дата обращения: 22.09.2022). — Режим доступа: для авториз. пользователей

Общие требования к организации практики

К прохождению производственной практики допускаются обучающиеся, не имеющие академической задолженности по междисциплинарным курсам и учебным практикам в рамках освоения профессионального модуля ПМ.03. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

Организация производственной практики осуществляется в сроки, установленные рабочим учебным планом, после изучения всего раздела междисциплинарного курса или чередуясь с темами теоретического обучения.

Максимальный объем производственной практики составляет 36 академических часов в неделю.

База практики должна соответствовать профилю специальности обучающегося.

На предприятии за студентом закрепляется руководитель, который проводит с ним инструктаж по технике безопасности, охране труда, знакомит обучающегося со структурой предприятия, помогает освоить темы производственной практики и осуществляет контроль ее прохождения. В колледже подготовкой обучающегося к производственной практике, консультацией по вопросам прохождения практики занимается заведующий практикой.

Во время прохождения практики обучающийся ведет дневник практики, в котором руководитель от предприятия делает отметки и выставляет оценки. В конце практикистудентоформляет отчет по производственной практике, согласно требованиям по составлению технического отчета. Руководитель практики от предприятия дает отзыв- характеристику о сформировавшихся у практиканта общих и профессиональных компетенциях, что учитывается в дальнейшем при получении итоговой оценки по практике.

Аттестация по итогам производственной практики (по профилю специальности) проводится с учетом результатов ее прохождения, подтверждаемых документами соответствующих организаций (баз практик). Студент должен представить в колледж для получения оценки по практике: технический отчет с выполненным заданием, заполненный дневник, аттестационный лист, который выдается студентам в колледже.

4. КОНТРОЛЬИОЦЕНКАРЕЗУЛЬТАТОВОСВОЕНИЯПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Одной из форм контроля результатов производственной практики является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

При оценивании отчета по практике учитываются оценка уровня прохождения производственной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Аттестация по итогам производственной практики – дифференцированный зачет - проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 3.1. Производить установку, монтаж, настройкуииспытания техническихсредствзащиты информации от утечки по техническим каналамвинформационно-телекоммуникационных системах и сетях.	-проводитьустановку,монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; -применятьнормативные правовыеактыинормативные методические документы в областизащиты информации;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания
ПК 3.2. Проводить техническоеобслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации,используемыхв информационно-телекоммуникационных системах и сетях.	- проводитьустановку,монтаж, настройку и испытание технических средств защиты информации от утечки потехническимканалам; - проводитьтехническое обслуживание, устранение неисправностей и ремонт техническихсредствзащиты информации от утечки по техническим каналам; - применятьнормативные правовые актыинормативные методические документывобластизащиты информации;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания

ПК3.3.Осуществлятьзащиту информации от утечки по техническим каналам в ИТКС с использованием техническихсредствзащиты в соответствии с предъявляемыми требованиями.	- проводитьизмерение параметров фоновых шумов и ПЭМИН, создаваемыхоборудованием ИТКС; - проводитьизмерение параметровэлектромагнитн ых излучений и токов, создаваемыхтехническими средствами защиты информациииотутечкипо техническим каналам; -применятьнормативные правовыеактыинормативные методические документы в областизащиты информации;	- наблюдение за действиямина практике - оценкадействийна практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть техническогоотчетапо выполнению индивидуальногозадания
ПК 3.4.Проводить отдельныеработыпо физическойзащителиний связиИТКС.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных(в том числе криптографических) средств защиты информации;	-наблюдение за действиями на практике -оценка действий на практике -оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.8
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности телекоммуникационных
систем

РАБОЧАЯ ПРОГРАММА
ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих
(14601 Монтажник оборудования связи)

СОДЕРЖАНИЕ

1. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

по профессиональным модулям ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи).

Область применения программы

Программа производственной практики по ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи), является частью образовательной программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части приобретения практического опыта в процессе освоения основного вида профессиональной деятельности (ВД): Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи и соответствующих профессиональных (ПК) и общих (ОК) компетенций:

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 4.	Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи)

Цели и задачи практики

Производственная практика в виде практической подготовки направлена на формирование у обучающихся умений, приобретение первоначального практического опыта и реализуется в рамках модулей ПООП (примерные основные образовательные программы) СПО по основным видам профессиональной деятельности для последующего освоения ими общих и профессиональных компетенций по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем: квалификация - техник по защите информации

Производственная практика базируется на междисциплинарных курсах профессионального модуля: МДК.04.01.Технология выполнения работ по профессии.

С целью освоения указанного вида профессиональной деятельности и соответствующих профессиональных компетенций в результате прохождения практической подготовки обучающийся должен:

Иметь практический опыт в	- забивки в грунт электродов заземления; - снятие и восстановление обшивки кабельных барабанов; - закрывание отверстий трубопровода с кабелем; - снятие джутового покрова с кабеля; - закрытие кабеля в траншеях кирпичом; - подготовка кабельных колодцев к прокладке (установка ограждений, открывание и закрывание колодцев и т.п.); установки деталей и арматуры для крепления и прокладки кабелей в шахтах, колодцах и по стенам; - установки кабельных барабанов на козла и домкраты; - разматывание кабелей, проводов, тросов при ручной прокладке; - установки замерных столбиков; - окраски и нумерация

уметь	- выполнять работы по прокладке линий связи; - выполнять работы по оборудованию вводов и прокладке кабельных линий связи.
знать	- виды материалов и конструкций, применяемых для крепления кабелей и проводов; - способы крепления и защиты кабелей от механических повреждений; - общие сведения по электросвязи; - марки кабелей связи; - правила обращения с кабелями; - правила пользования механизированным инструментом; - способы включения телефонных аппаратов и батарей питания; - способы защиты кабелей от ударов молнии и коррозии; - конструкции кабелей связи; - виды повреждений кабелей и способы их отыскания; - методы проверки кабелей на герметичность, обрыв, землю и сообщение; - способы и средства для прокладки кабелей, проводов и тросов; - схемы организаций линий связи; - организацию и технологию работ по прокладке кабелей в земле и кабельной канализации; - машины и механизмы для прокладки кабелей; - организацию и технологию работ по прокладке кабелей в сложных условиях.

Количество часов на освоение программы производственной практики (по профилю специальности)

ПП.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи):
производственная практика (по профилю специальности) по ПМ.04. –144 часов.
Форма промежуточной аттестации–дифференцированный зачет.

Результатом освоения программы учебной и производственной практики профессионального модуля ПМ.04. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (14601 Монтажник оборудования связи) является овладение профессиональными (ПК) и общими (ОК) компетенциями:

Код компетенции	**Наименование результата обучения**
ПК 1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно - телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно - телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно - телекоммуникационных систем и сетей

ПК 1.4.	Осуществлять контроль функционирования информационно - телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно - телекоммуникационных систем и сетей
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно - телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно - телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно - телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно - телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно - телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно - телекоммуникационных систем и сетей
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

№ п/п	Разделы (этапы) практики	Содержание разделов (этапов) практики	Количество часов
1.	Организационные вопросы оформления на предприятии, установочная лекция, инструктаж по охране труда и технике безопасности, распределение по рабочим местам	- Изучение инструкции по охране труда. - Изучение инструкции по технике безопасности и пожаробезопасности, схем аварийных проходов и выходов, пожарного инвентаря. - Изучение правил внутреннего распорядка. - Изучение правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	36
2.	Ознакомление со структурой и характером деятельности предприятия	1. Знакомство со штатным расписанием 2. Знакомство с отделами организации 3. Знакомство с видами деятельности отделов организации	20
3.	Обзор типовых задач, которые решаются на производстве. Ознакомление с программным обеспечением, которое используется на предприятии. Работа с программным обеспечением компьютерной системы. Ознакомление с оборудованием Изучение системы защиты информации на предприятии	Должностные инструкции работников отдела, подразделения предприятия. Подготовка к работе вычислительной техники и периферийных устройств. Настройка параметров функционирования персонального компьютера, периферийного оборудования и компьютерной техники Работа с физическими носителями и накопителями информации. Работа с сетевыми и облачными накопителями информации. Ввод цифровой и аналоговой информации в персональный компьютер с различных носителей, периферийного и мультимедийного оборудования Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники. Изучение элементов и схемы защиты Защита паролем. Защита элементов листа. Использование Центра управления безопасностью. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных. Выполнение резервного копирования и восстановления данных. Внешние влияния и способы защиты. Источник опасных и мешающих влияний. Нормы опасных и мешающих влияний.	64

		Электромонтажные работы. Подготовка кабелей к прокладке. Выполнение работ по прокладке кабельных линий связи Принципы монтажа кабелей. Принципы монтажа кабелей местных телефонных сетей, междугородных, симметричных и коаксиальных кабелей. Особенности монтажа оптических кабелей.	
4.	Оформление отчета о прохождении производственной практики (преддипломной)	Оформление отчета в соответствии с требованиями	18
5.		Сдача технического отчета по производственной (преддипломной) практике	6
		Всего часов	**144**

1. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ

Требования к минимальному материально-техническому обеспечению
Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся:

ООО «ФАБРИКА «ДОНБАСС-ЛИБЕРТИ»
Реализация рабочей программы производственной практики предусмотрены следующие специальные помещения: участок металлической мебели мебельного производства.
Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.
Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.
Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.
Локальная сеть с выходом в Интернет.

ФИЛИАЛ № 1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВАОД «СИЛУР» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РОСТЭКСПОСНАБ 8»
Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта.
Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.
Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.
Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.
Локальная сеть с выходом в Интернет.

Информационное обеспечение реализации программы

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение 180ЯЕС 154082:2008). Росстандарт, 2013.

42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

45. Требования о защите информации, не составляющей государственную тайну,

содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2020.

2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учрежд. СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.

3. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.

4. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.

5. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018.

6. Заика, А.А. Локальные сети и Интернет/ А.А. Заика. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

7. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. - 7-е изд., испр. - Москва: Горячая Линия-Телеком, 2018.

8. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.

9. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2018.

10. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва: Юрайт, 2020.

11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.

12. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2020.

13. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков. - Москва: Горячая Линия-Телеком, 2017.

14. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов/В.Г.Олифер, Н.А.Олифер. - С.-Петербург: Питер, 2018.

15. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2020.

16. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012.

17. Программно-аппаратные средства обеспечения информационной безопасности/ А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. - Москва: Горячая Линия-Телеком, 2016.

18. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: учебное пособие для вузов/Е.Б.Алексеев, В.Н.Гордиенко, В.В.Крухмалев и др.; под ред. В.Н.Гордиенко, М.С.Тверецкого. - Москва: Горячая линия-Телеком, 2017.

19. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016.

20. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва: ЮРАЙТ, 2020.

21. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. -2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019.

22. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. - М.: Инфра-Инженерия, 2019.

23. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. -2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020.

24. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. - Москва: Инфра-Инженерия, 2019.

25. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020.

26. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - М.: ФОРУМ: ИНФРА-М, 2020.

Электронные ресурсы:

1. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". – URL: http://www.securitylab.ru

2. Андрончик, А. Н. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. –URL: http://elar.urfu.ru/handle/10995/28990.

3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.– Текст: электронный. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL:http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf.

4. Жданов, О. Криптографические методы защиты информации/О.Жданов, Ю.Ушаков. - Москва: ИНТУИТ, 2016. – URL:https://www.intuit.ru/studies/courses/13837/1234/info.

5. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности/Г.П.Жигулин; НИУ ИТМО. – С.-Петербург: НИУ ИТМО, 2014.– URL:https://books.ifmo.ru/file/pdf/1484.pdf.

6. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие/ Н.С.Кармановский, О.В.Михайличенко, Н.Н.Прохожев. –С.-Петербург: НИУ ИТМО, 2016. – URL: https://books.ifmo.ru/file/pdf/1093.pdf.

7. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие /Ю.Ф.Каторин, А.В.Разумовский, А.И.Спивак; под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf.

8. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин.– Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006.–

URL:https://tstu.ru/book/elib/pdf/2006/shamkin1.pdf/.

9. Маркина, Т.А. Средства защиты вычислительных систем и сетей: учебное пособие/Т.А.Маркина; НИУ ИТМО.– С.-Петербург: Университет ИТМО, 2016.-URL: https://books.ifmo.ru/file/pdf/2121.pdf.

10. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - Москва: Национальный Открытый Университет ИНТУИТ. – URL:https://www.intuit.ru/studies/courses/4/102/info.

11. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Часть 1: Методическая разработка /А.П.Пленкин, Ю.В.Зачиняев. URL: http://open-edu.rsu.ru/files/Методичка%20№4.pdf.

12. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Оптическое волокно. Часть 2: Методическая разработка/А.П.Пленкин. –Таганрог, 2016. – URL: http://openedu.rsu.ru/files/Методичка%20№5.pdf.

13. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. –2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL:https://books.ifmo.ru/file/pdf/2372.pdf.

14. Техническая эксплуатация линейных сооружений: учебное пособие/ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»; Колледж связи. – Самара, 2017. – URL: http://ks.psuti.ru/downloads/students/distance_learning/3МТС74,75/МДК.В.01.05%20Техническая%20эксплуатация%20линейных%20сооружений/МДК.01.05%20Учебное%20пособие.pdf.

15. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm.

Дополнительные источники:

1. Андреев, В.А. Направляющие системы электросвязи: учебник для вузов. В 2 т. Т.1. Теория передачи и влияния/ В.А.Андреев, Э.Л.Портнов, Л.Н.Кочановский. - Москва: Горячая линия-Телеком, 2011.

2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013.

3. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.

4. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.

5. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия-Телеком, 2012.

6. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. -Москва: Горячая линия-Телеком, 2013.

7. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012.

8. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков. - М.: ТУСУР, 2016.

9. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019.

10. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - М.: СОЛОН-Пресс, 2013.

11. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие

/ А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017.

12. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом: учебное пособие / Н.Б. Ельчанинова; Южный федеральный университет. - Ростов-на-Дону - Таганрог: Издательство Южного федерального университета, 2017.

13. Запечников, С. В. Основы построения виртуальных частных сетей: учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва: Гор. линия-Телеком, 2011.

14. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.

15. Кенин, А.М. Практическое руководство системного администратора /А.М.Кенин. - С.Петербург: БХВ-Петербург, 2013.

16. Кенин, А.М. Самоучитель системного администратора / А.М.Кенин, Д.Н.Колисниченко. - 4-е изд., перераб. и доп. - С.-Петербург: БХВ-Петербург, 2016.

17. Лапонина, О.Р. Межсетевое экранирование: учебное пособие / О.Р. Лапонина. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2017.

18. Метрология и электрорадиоизмерения в телекоммуникационных системах: учебное пособие / С.И. Боридько, Н.В. Дементьев и др.; под общ. ред. Б.Н. Тихонова - 2 изд., стер. - Москва: Горячая линия-Телеком, 2012.

19. Направляющие системы электросвязи . В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация : учебник для ВУЗов /В.А.Андреев, А.В.Бурдин, Л.Н.Кочановский и др.; под ред. В.А.Андреева. - М.: Горячая линия-Телеком, 2010.

20. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013.

21. Портнов, Э.Л. Электрические кабели связи и их монтаж: учебное пособие/Э.Л.Портнов, А.Л.Зубилевич. - 2-е изд. - Москва: Горячая линия-Телеком, 2010.

22. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - М.: Горячая линия-Телеком, 2014.

23. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — Москва: Форум: ИНФРА-М, 2020.

24. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. - Москва: Горячая линия-Телеком, 2017.

25. Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - 2-е изд. - Москва: Гор. линия-Телеком, 2016.

26. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013.

27. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

28. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей Р^Н, 8^Н, 1Р, ЕШете! и АТМ/И.И. Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - Москва: Горячая линия-Телеком, 2017.

29. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

30. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: учебник для студ. учрежд. СПО/Е.Л.Чащина. - Москва: Академия, 2016.

31. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров,

серверов, периферийных устройств, оборудования и компьютерной оргтехники: практикум: учебное пособие для студ. учрежд. СПО/Е.Л.Чащина. - Москва: Академия, 2016.

32. Чернышев, Е.И. Линейные сооружения связи: учебное пособие для студ. учрежд. СПО/Е.И.Чернышев. - Волгоград: Ин-Фолио, 2010.

33. Электрорадио измерения: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов, В.К.Битюков, Е.В.Самохина; под ред. А.С.Сигова. - Москва: Форум: Инфра-М, 2020.

4. КОНТРОЛЬИОЦЕНКАРЕЗУЛЬТАТОВОСВОЕНИЯПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПО ПРОФИЛЮ СПЕЦИАЛЬНОСТИ)

Одной из форм контроля результатов производственной практики является дневник практики, который ведется обучающимся в процессе прохождения практики.

По результатам прохождения производственной практики обучающийся составляет технический отчет, который утверждается организацией, на базе которой проходила практика. В качестве приложения к дневнику практики обучающийся оформляет материалы по индивидуальному заданию на практику, а так же графические, аудио-, фото-, видео-, материалы, подтверждающие практический опыт, полученный на практике.

При оценивании отчета по практике учитываются оценка уровня прохождения производственной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Аттестация по итогам производственной практики – дифференцированный зачет - проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования ИТКС	– осуществлять техническую эксплуатацию линейных сооружений связи; – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; – измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.3. Проводить техническое обслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений ИТКС; - измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики,

	- производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.4. Осуществлять контроль функционирования ИТКС	- проводить мониторинг и контроль функционирования оборудования ИТКС; - измерять основные параметры и характеристики оборудования ИТКС; - вести эксплуатационно-техническую документацию на оборудование ИТКС;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; – проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; – проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно- аппаратных (в том числе криптографических) средств	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
	защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.	-проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в пониманиии изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.

Приложение 4.9
к ОПОП по специальности 10.02.04
Обеспечение информационной
безопасности телекоммуникационных
систем

РАБОЧАЯ ПРОГРАММА ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

СПЕЦИАЛЬНОСТИ 10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

СОДЕРЖАНИЕ

2. ПАСПОРТ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Область применения программы

Программа производственной практики (преддипломной) является обязательной частью профессионального цикла образовательной программы в соответствии с ФГОС СПО по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем как заключительного этапа подготовки студентов по указанной специальности к самостоятельной практической деятельности по видам деятельности (ВД).

Программа производственной практики (преддипломной) может быть использована в дополнительном профессиональном образовании, в программах повышения квалификации и переподготовки работников в области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии, 12 обеспечение безопасности.

В рамках освоения видов деятельности у выпускника должны быть сформированы соответствующие профессиональные (ПК) компетенции и соответствующие им практический опыт, умения и знания.

Производственная практика (преддипломная) базируется на междисциплинарных курсах профессиональных модулей:

- ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей
- МДК.01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания
- МДК.01.02. Телекоммуникационные системы и сети
- МДК.01.03. Электрорадиоизмерения и метрология
- ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных в том числе, криптографических средств защиты
- МДК.02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты
- МДК.02.02. Криптографическая защита информации
- ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты
- МДК.03.01.Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты
- МДК.03.02.Физическая защита линий связи информационно-телекоммуникационных систем и сетей

Цели и задачи практики

Цель производственной практики (преддипломной) – обобщение и совершенствование знаний и умений студентов по специальности, проверка возможности самостоятельной работы будущего специалиста в условиях конкретного предприятия, получение необходимых материалов для выполнения выпускаемой квалификационной работы.

К задачам преддипломной практики относятся: - закрепление теоретических знаний, полученных студентами в процессе обучения, на основе знакомства с опытом работы конкретного предприятия (организации), в области производственной деятельности.

В результате прохождения производственной практики обучающийся должен освоить основной вид деятельности, общие компетенции, профессиональные компетенции и соответствующие им знания, умения и навыки.

Задачи:

- овладение профессиональной деятельностью, развитие профессионального мышления;
- закрепление, углубление, расширение и систематизация знаний, закрепление практических навыков и умений, полученных при изучении дисциплин и профессиональных модулей, определяющих специфику специальности;
- обучение навыкам решения практических задач при подготовке к итоговой аттестации;
- проверка профессиональной готовности к самостоятельной трудовой деятельности выпускника.

Для освоения программы производственной практики (преддипломной) студент должен иметь практический опыт, полученный в результате освоения междисциплинарных курсов профессиональных модулей по видам деятельности.

Основной вид деятельности	**Умения и практический опыт**
Эксплуатация информационно-телекоммуникационных систем и сетей	монтаж, настройка, проверка функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (далее - ИТКС);
	текущий контроль функционирования оборудования ИТКС; диагностика технического состояния приёмо-передающих устройств и линейных сооружений связи и источников питания;
	проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта оборудования ИТКС;
	текущий контроль функционирования оборудования ИТКС; мониторинг технического состояния и работоспособности приёмо-передающих устройств и линейных сооружений связи и источников питания ИТКС;
Защита информации в информационно-телекоммуникационных системах и сетях с использованием программно-аппаратных, в том числе криптографических средств защиты	установка, настройка, испытаний и конфигурирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;
	поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС
	защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями;
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам
	установка, монтаж, настройка и испытание технических средств защиты информации от утечки по техническим каналам; проведение технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
	защита информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации;
Защита информации в информационно телекоммуникационных системах и сетях с использованием	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам;

технических средств защиты	проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС;
	проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам;
	применять нормативные правовые акты и нормативные методические документы в области защиты информации;
	применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных
	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам;
	установки, монтажа, настройки и испытаний технических средств защиты информации от утечки по техническим каналам; проведения технического обслуживания и ремонта технических средств защиты информации от утечки по техническим каналам;
	защиты информации от утечки по техническим каналам с использованием технических средств защиты в соответствии с предъявляемыми требованиями;
	проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; выявление технических каналов утечки информации

Количество часов на освоение рабочей программы производственной практики (преддипломной):

В рамках освоения продолжительность производственной практики (преддипломной) 144 часа.

Промежуточная аттестация в форме дифференцированного зачёта.

РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Результатом освоения рабочей программы производственной практики (преддипломной) является углубление практического опыта обучающихся, развитие общих и профессиональных компетенций, готовность к самостоятельной трудовой деятельности.

Код	**Наименование компетенции**
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 09	Использовать информационные технологии в профессиональной деятельности
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языках
ОК 11	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере
ПК1.1.	Производить монтаж, настройку и поверку функционирования и конфигурирования оборудования информационно - телекоммуникационных систем и сетей.
ПК 1.2.	Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования информационно - телекоммуникационных систем и сетей.
ПК 1.3.	Проводить техническое обслуживание оборудования информационно - телекоммуникационных систем и сетей
ПК 1.4.	Осуществлять контроль функционирования информационно - телекоммуникационных систем и сетей
ПК 2.1.	Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно - телекоммуникационных систем и сетей

Код	Наименование компетенции
ПК 2.2.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно - телекоммуникационных системах и сетях
ПК 2.3.	Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно - телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями.
ПК 3.1.	Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно - телекоммуникационных системах и сетях.
ПК 3.2.	Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно - телекоммуникационных системах и сетях
ПК 3.3.	Осуществлять защиту информации от утечки по техническим каналам в информационно - телекоммуникационных системах и сетях с использованием технических средств защиты в соответствии с предъявляемыми требованиями.
ПК 3.4.	Проводить отдельные работы по физической защите линий связи информационно - телекоммуникационных систем и сетей

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

№ п/п	Разделы (этапы) практики	Содержание разделов (этапов) практики	Количество часов
1.	Организационные вопросы оформления на предприятии, установочная лекция, инструктаж по охране труда и технике безопасности, распределение по рабочим местам	- Изучение инструкции по охране труда. - Изучение инструкции по технике безопасности и пожаробезопасности, схем аварийных проходов и выходов, пожарного инвентаря. - Изучение правил внутреннего распорядка. - Изучение правил и норм охраны труда, техники безопасности при работе с вычислительной техникой.	36
2.	Ознакомление со структурой и характером деятельности предприятия	4. Знакомство со штатным расписанием 5. Знакомство с отделами организации 6. Знакомство с видами деятельности отделов организации	36
3.	Сбор материалов для составления технического задания по теме дипломного проекта и сдаче демонстрационного экзамена.	1. Подготовка списка источников 2. Изучение нормативных документов 3. Составление плана 4. Изучение технической документации	48
4.	Оформление отчета о прохождении производственной практики (преддипломной)	Оформление отчета в соответствии с требованиями	18
5.		Сдача технического отчета по производственной (преддипломной) практике	6
		Всего часов	**144**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Требования к минимальному материально-техническому обеспечению
Реализация программы предполагает проведение производственной практики на предприятиях/организациях на основе прямых договоров, заключаемых между образовательным учреждением и каждым предприятием/организацией, куда направляются обучающиеся:

ООО «ФАБРИКА «ДОНБАСС-ЛИБЕРТИ»
Реализация рабочей программы производственной практики предусмотрены следующие специальные помещения: участок металлической мебели мебельного производства.
Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.
Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.
Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.
Локальная сеть с выходом в Интернет.

ФИЛИАЛ № 1 «ХАРЦЫЗСКИЙ СТАЛЕПРОВОЛОЧНЫЙ-КАНАТНЫЙ ЗАВАОД «СИЛУР» ОБЩЕСТВА С ОГРАНИЧЕННОЙ ОТВЕТСТВЕННОСТЬЮ «РОСТЭКСПОСНАБ 8»
Для прохождения производственной практики на предприятиях организованы технически оснащенные рабочие места практиканта.
Основное оборудование: офисная мебель, посадочные места по количеству обучающихся, наглядные пособия, комплект нормативных документов.
Технические средства обучения: персональные компьютеры, ноутбуки, оргтехника, МФУ.
Программное обеспечение: Операционная система, офисный пакет, специализированное программное обеспечение систем приема, передачи и обработки сигналов.
Локальная сеть с выходом в Интернет.

Информационное обеспечение реализации программы

Нормативные документы:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

3. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

4. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

5. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-

телекоммуникационных сетей международного информационного обмена».

9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.

11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.

12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.

15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

16. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

17. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

18. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

19. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638.

20. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

21. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий

24. ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25. ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

27. ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

28. ГОСТ Р ИСО/МЭК 15408-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель

29. ГОСТ Р ИСО/МЭК 15408-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности

30. ГОСТ Р ИСО/МЭК 15408-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности

31. ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

32. ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

33. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

34. ГОСТ Р 52069.0-2013 Защита информации. Система стандартов. Основные положения. Росстандарт, 2013.

35. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

36. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

37. ГОСТ Р 52447-2005 Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

39. ГОСТ Р 56115-2014 Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

40. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

41. ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение 180ЯЕС 154082:2008). Росстандарт, 2013.

42. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

43. Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

44. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

45. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11

февраля 2013 г. № 17.

46. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

47. Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

Электронные издания:

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие/ Е.К.Баранова, А.В.Бабаш. — 3-е изд., перераб. и доп. — М.: РИОР: ИНФРА-М, 2020.

2. Баранова, Е.К. Основы информационной безопасности: учебник для студ. учрежд. СПО / Е.К. Баранова, А.В. Бабаш. - М.: РИОР: ИНФРА-М, 2019.

3. Берлин, А. Н. Высокоскоростные сети связи: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.

4. Берлин, А. Н. Оконечные устройства и линии абонентского участка информационной сети: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.

5. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам: учебное пособие для вузов/Г.А.Бузов. - Москва: Горячая линия-Телеком, 2018.

6. Заика, А.А. Локальные сети и Интернет/ А.А. Заика. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

7. Зайцев, А. П. Технические средства и методы защиты информации: учебник для вузов / А.П.Зайцев, Р.В.Мещеряков, А.А.Шелупанов. - 7-е изд., испр. - Москва: Горячая Линия-Телеком, 2018.

8. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.

9. Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие для студ. учрежд. СПО /В.Я.Ищейнов, М.В.Мецатунян. - Москва: Форум: ИНФРА-М, 2018.

10. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. - Москва: Юрайт, 2020.

11. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения: учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. - Москва: Юрайт, 2020.

12. Криптографическая защита информации: учебное пособие / С.О. Крамаров, О.Ю. Митясова, С В. Соколов [и др.]; под ред. проф. С.О. Крамарова. — Москва: РИОР: ИНФРА-М, 2020.

13. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации): учебное пособие / В.К. Новиков. - Москва: Горячая Линия-Телеком, 2017.

14. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов/В.Г.Олифер, Н.А.Олифер. - С.-Петербург: Питер, 2018.

15. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; под ред. Т. А. Поляковой, А. А. Стрельцова. — Москва: Юрайт, 2020.

16. Портнов, Э. Л. Оптические кабели связи, их монтаж и измерение: учебное пособие для вузов / Э.Л. Портнов. - Москва: Горячая линия-Телеком, 2012.

17. Программно-аппаратные средства обеспечения информационной безопасности/

А.В.Душкин, О.М.Барсуков, Е.В.Кравцов, К.В.Славнов. - Москва: Горячая Линия-Телеком, 2016.

18. Проектирование и техническая эксплуатация цифровых телекоммуникационных систем и сетей: учебное пособие для вузов/Е.Б.Алексеев, В.Н.Гордиенко, В.В.Крухмалев и др.; под ред. В.Н.Гордиенко, М.С.Тверецкого. - Москва: Горячая линия-Телеком, 2017.

19. Родина, О.В. Волоконно-оптические линии связи: практическое руководство/О.В.Родина. - Москва: Горячая линия-Телеком, 2016.

20. Сети и телекоммуникации: учебник и практикум для среднего профессионального образования / К. Е. Самуйлов [и др.]; под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. - Москва: ЮРАЙТ, 2020.

21. Смычек, М.А. Технологические сети и системы связи: учебное пособие / М.А. Смычек. -2-е изд. - Москва; Вологда: Инфра-Инженерия, 2019.

22. Соколов, С.А. Волоконно-оптические линии связи и их защита от внешних влияний: учебное пособие / С.А. Соколов. - М.: Инфра-Инженерия, 2019.

23. Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие/П.Б.Хорев. -2-е изд., испр. и доп. - Москва: Форум: ИНФРА-М, 2020.

24. Цуканов, В.Н. Волоконно-оптическая техника: практическое руководство/ В.Н. Цуканов, М.Я. Яковлев. - Москва: Инфра-Инженерия, 2019.

25. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В.Ф. Шаньгин. - Москва: ФОРУМ: ИНФРА-М, 2020.

26. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учебное пособие для студ. учрежд. СПО. - М.: ФОРУМ: ИНФРА-М, 2020.

Электронные ресурсы:

1. SecurityLab. Защита информации и информационная безопасность: информационный портал/ООО "PositiveTechnologies". – URL: http://www.securitylab.ru

2. Андрончик, А. Н. Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие / А. Н. Андрончик, А. С. Коллеров, Н. И. Синадский, М. Ю. Щербаков; под общ. ред. Н. И. Синадского. –URL: http://elar.urfu.ru/handle/10995/28990.

3. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.– Текст: электронный. - Екатеринбург: Изд-во Урал. ун-та, 2019. – URL:http://elar.urfu.ru/bitstream/10995/73899/3/978-5-7996-2677-8_2019.pdf.

4. Жданов, О. Криптографические методы защиты информации/О.Жданов, Ю.Ушаков. - Москва: ИНТУИТ, 2016. – URL:https://www.intuit.ru/studies/courses/13837/1234/info.

5. Жигулин, Г.П. Организационное и правовое обеспечение информационной безопасности/Г.П.Жигулин; НИУ ИТМО. – С.-Петербург: НИУ ИТМО, 2014.– URL:https://books.ifmo.ru/file/pdf/1484.pdf.

6. Кармановский, Н.С. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие/ Н.С.Кармановский, О.В.Михайличенко, Н.Н.Прохожев. –С.-Петербург: НИУ ИТМО, 2016. – URL: https://books.ifmo.ru/file/pdf/1093.pdf.

7. Каторин, Ю.Ф. Защита информации техническими средствами: учебное пособие /Ю.Ф.Каторин, А.В.Разумовский, А.И.Спивак; под редакцией Ю.Ф. Каторина. – С.-Петербург: НИУ ИТМО, 2012. – URL: https://books.ifmo.ru/file/pdf/975.pdf.

8. Криптографическая защита информации: учебное пособие / А.В. Яковлев, А.А. Безбогов, В.В. Родин, В.Н. Шамкин.– Тамбов: Изд-во Тамб. гос. техн. ун-та, 2006.– URL:https://tstu.ru/book/elib/pdf/2006/shamkin1.pdf/.

9. Маркина, Т.А. Средства защиты вычислительных систем и сетей: учебное

пособие/Т.А.Маркина; НИУ ИТМО.– С.-Петербург: Университет ИТМО, 2016.-URL: https://books.ifmo.ru/file/pdf/2121.pdf.

10. Мэйволд, Э. Безопасность сетей / Э. Мэйволд. - Москва: Национальный Открытый Университет ИНТУИТ. – URL:https://www.intuit.ru/studies/courses/4/102/info.

11. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Часть 1: Методическая разработка /А.П.Пленкин, Ю.В.Зачиняев. URL: http://open-edu.rsu.ru/files/Методичка%20№4.pdf.

12. Пленкин, А.П. Построение, измерения и тестирование проводных линий связи телекоммуникационной сети. Оптическое волокно. Часть 2: Методическая разработка/А.П.Пленкин. –Таганрог, 2016. – URL: http://openedu.rsu.ru/files/Методичка%20№5.pdf.

13. Теория информационной безопасности и методология защиты информации /Ю.А.Гатчин, В.В.Сухостат, А.С.Куракин, Ю.В.Донецкая. –2-е изд., испр. и доп. – С.-Петербург: Университет ИТМО, 2018. – URL:https://books.ifmo.ru/file/pdf/2372.pdf.

14. Техническая эксплуатация линейных сооружений: учебное пособие/ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики»; Колледж связи. – Самара, 2017. – URL: http://ks.psuti.ru/downloads/students/distance_learning/3MTC74,75/МДК.В.01.05%20Техническая%20эксплуатация%20линейных%20сооружений/МДК.01.05%20Учебное%20пособие.pdf.

15. Энциклопедия инструментов: иллюстрированный справочник по инструментам и приборам. – URL: http://www.tools.ru/tools.htm.

Дополнительные источники:

1. Андреев, В.А. Направляющие системы электросвязи: учебник для вузов. В 2 т. Т.1. Теория передачи и влияния/ В.А.Андреев, Э.Л.Портнов, Л.Н.Кочановский. - Москва: Горячая линия-Телеком, 2011.

2. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013.

3. Берлин, А. Н. Абонентские сети доступа и технологии высокоскоростных сетей: учебное пособие / А. Н. Берлин. — 2-е изд. — Москва: ИНТУИТ, 2016.

4. Берлин, А. Н. Телекоммуникационные сети и устройства: учебное пособие / А. Н. Берлин. - 2-е изд. - Москва: ИНТУИТ, 2016.

5. Ворона, В. А. Инженерно-техническая и пожарная защита объектов / В.А. Ворона, В.А. Тихонов. - Москва: Горячая Линия-Телеком, 2012.

6. Ворона, В.А. Системы контроля и управления доступом/В.А.Ворона, В.А.Тихонов. -Москва: Горячая линия-Телеком, 2013.

7. Ворона, В.А. Технические системы охранной и пожарной сигнализации /В.А.Ворона, В.А.Тихонов. - Москва: Горячая линия-Телеком, 2012.

8. Голиков, А.М. Тестирование и диагностика в инфокоммуникационных системах и сетях: учебное пособие / А.М. Голиков. - М.: ТУСУР, 2016.

9. Гришина, Н.В. Информационная безопасность предприятия: учебное пособие/Н.В.Гришина. - 2-е изд., доп. - Москва: Форум: ИНФРА-М, 2019.

10. Груба, И.И. Системы охранной сигнализации. Технические средства обнаружения: справочное пособие / И.И.Груба. - М.: СОЛОН-Пресс, 2013.

11. Душкин, А.В. Аппаратные и программные средства защиты информации: учебное пособие / А.В.Душкин, А.Кольцов, А.Кравченко. - Воронеж: Научная книга, 2017.

12. Ельчанинова, Н.Б. Правовые основы защиты информации с ограниченным доступом:

учебное пособие / Н.Б. Ельчанинова; Южный федеральный университет. - Ростов-на-Дону - Таганрог: Издательство Южного федерального университета, 2017.

13. Запечников, С. В. Основы построения виртуальных частных сетей: учебное пособие для вузов / С.В. Запечников, Н.Г. Милославская, А.И. Толстой. - Москва: Гор. линия-Телеком, 2011.

14. Защита информации: учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 3-е изд. - Москва: РИОР: ИНФРА-М, 2019.

15. Кенин, А.М. Практическое руководство системного администратора /А.М.Кенин. - С.Петербург: БХВ-Петербург, 2013.

16. Кенин, А.М. Самоучитель системного администратора / А.М.Кенин, Д.Н.Колисниченко. -4-е изд., перераб. и доп. - С.-Петербург: БХВ-Петербург, 2016.

17. Лапонина, О.Р. Межсетевое экранирование: учебное пособие / О.Р. Лапонина. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2017.

18. Метрология и электрорадиоизмерения в телекоммуникационных системах: учебное пособие / С.И. Боридько, Н.В. Дементьев и др.; под общ. ред. Б.Н. Тихонова - 2 изд., стер. - Москва: Горячая линия-Телеком, 2012.

19. Направляющие системы электросвязи . В 2-х т. Т. 2. Проектирование, строительство и техническая эксплуатация : учебник для ВУЗов /В.А.Андреев, А.В.Бурдин, Л.Н.Кочановский и др.; под ред. В.А.Андреева. - М.: Горячая линия-Телеком, 2010.

20. Портнов, Э. Л. Принципы построения первичных сетей и оптические кабельные линии связи: учебное пособие для вузов / Э.Л.Портнов. - Москва: Горячая линия-Телеком, 2013.

21. Портнов, Э.Л. Электрические кабели связи и их монтаж: учебное пособие/Э.Л.Портнов, А.Л.Зубилевич. - 2-е изд. - Москва: Горячая линия-Телеком, 2010.

22. Проскурин, В.Г. Защита в операционных системах: учебное пособие для вузов/В.Г.Проскурин. - М.: Горячая линия-Телеком, 2014.

23. Романьков, В.А. Введение в криптографию: курс лекций / В.А. Романьков. - 2-е изд., испр. и доп. — Москва: Форум: ИНФРА-М, 2020.

24. Рябко, Б. Я. Криптографические методы защиты информации: учебное пособие/ Б.Я.Рябко, А.Н.Фионов. - Москва: Горячая линия-Телеком, 2017.

25. Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я.Рябко, А.Н.Фионов. - 2-е изд. - Москва: Гор. линия-Телеком, 2016.

26. Субботин, Е. А. Методы и средства измерения параметров оптических телекоммуникационных систем: учебное пособие для вузов / Е.А. Субботин. - Москва: Горячая линия-Телеком, 2013.

27. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

28. Техническая диагностика современных цифровых сетей связи. Основные принципы и технические средства измерений параметров передачи для сетей Р^Н, 8^Н, 1Р, ЕШете! и АТМ/И.И. Власов, Э.В.Новиков, М.М.Птичников, Д.В.Сладких; под ред. М.М.Птичникова. - Москва: Горячая линия-Телеком, 2017.

29. Технологии защиты информации в компьютерных сетях / Н.А. Руденков [и др.]. - М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.

30. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: учебник для студ. учрежд. СПО/Е.Л.Чащина. - Москва: Академия, 2016.

31. Чащина, Е.Л. Обслуживание аппаратного обеспечения персональных компьютеров, серверов, периферийных устройств, оборудования и компьютерной оргтехники: практикум: учебное пособие для студ. учрежд. СПО/Е.Л.Чащина. - Москва: Академия, 2016.

32. Чернышев, Е.И. Линейные сооружения связи: учебное пособие для студ. учрежд.

СПО/Е.И.Чернышев. - Волгоград: Ин-Фолио, 2010.

33. Электрорадио измерения: учебник для студ. учрежд. СПО /В.И.Нефедов, А.С.Сигов, В.К.Битюков, Е.В.Самохина; под ред. А.С.Сигова. - Москва: Форум: Инфра-М, 2020.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОИЗВОДСТВЕННОЙ ПРАКТИКИ (ПРЕДДИПЛОМНОЙ)

Контроль и оценка результатов освоения учебной практики осуществляется руководителем практики в процессе проведения практики и приёма отчетов, а также сдачи обучающимися дифференцированного зачета.

При оценивании отчета по практике учитываются оценка уровня прохождения производственной практики; оценка компетенций; практических профессиональных умений, обучающихся при проведении видов работ.

Аттестация по итогам производственной практики – дифференцированный зачет - проводится с учетом (или на основании) результатов, подтвержденных документами соответствующих организаций.

Результаты (освоенные ПК)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить монтаж, настройку, проверку функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей	- производить монтаж кабельных линий и оконечных кабельных устройств ИТКС; - проверять функционирование, производить регулировку и контроль основных параметров источников питания ИТКС; - измерять основные показатели и характеристики при выполнении работ по настройке, проверке функционирования и конфигурирования ИТКС;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.2. Осуществлять диагностику технического состояния, поиск неисправностей и ремонт оборудования ИТКС	– осуществлять техническую эксплуатацию линейных сооружений связи; – проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; – измерять основные параметры и характеристики при выполнении работ по диагностике технического состояния, поиска неисправностей и ремонте оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.3. Проводить техническое обслуживание оборудования ИТКС	- осуществлять техническую эксплуатацию линейных сооружений ИТКС; - измерять основные параметры и характеристики при выполнении технического обслуживания оборудования ИТКС;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики,

	- производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 1.4. Осуществлять контроль функционирования ИТКС	- проводить мониторинг и контроль функционирования оборудования ИТКС; - измерять основные параметры и характеристики оборудования ИТКС; - вести эксплуатационно-техническую документацию на оборудование ИТКС;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.1. Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных систем и сетей.	– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; – проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации; – проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 2.2. Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - проводить контроль показателей и процесса функционирования программных и программно- аппаратных (в том числе криптографических) средств защиты информации; - проводить восстановление процесса и параметров функционирования программных и программно- аппаратных (в том числе криптографических) средств	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
	защиты информации; - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;	

ПК 2.3. Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно-телекоммуникационных системах и сетях с использованием программных и программно- аппаратных, в том числе криптографических средств в соответствии с предъявляемыми требованиями.	- выявлять и оценивать угрозы безопасности информации в ИТКС; - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; - проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в информационно-телекоммуникационных системах и сетях.	-проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	– наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в информационно-телекоммуникационных системах и сетях.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания
ПК 3.3. Осуществлять защиту информации от утечки по техническим каналам в ИТКС с использованием технических средств защиты в соответствии с предъявляемыми требованиями.	- проводить измерение параметров фоновых шумов и ПЭМИН, создаваемых оборудованием ИТКС; - проводить измерение параметров электромагнитных излучений и токов, создаваемых техническими средствами защиты информации от утечки по техническим каналам; применять нормативные правовые акты и нормативные методические документы в области защиты информации;	- наблюдение за действиями на практике – оценка действий на практике – оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

ПК 3.4. Проводить отдельные работы по физической защите линий связи ИТКС.	– выявлять и оценивать угрозы безопасности информации в ИТКС; – настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты; проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;	- наблюдение за действиями на практике - оценка действий на практике - оценка результатов дифференцированного зачета Дневник практики, Аттестационный лист, описательная часть технического отчета по выполнению индивидуального задания

Критерии оценки дифференцируемого зачета

Оценка «5» - «отлично» выставляется обучающемуся, если демонстрируются всестороннее, систематическое и глубокое знание учебного программного материала, самостоятельно выполнивший все предусмотренные программой задания, глубоко усвоивший основную и дополнительную литературу, рекомендованную программой, активно работавший на практических занятиях, разбирающийся в основных научных концепциях по изучаемой дисциплине, проявивший творческие способности и научный подход в понимании и изложении учебного программного материма, ответ отличается богатством и точностью использованных терминов, материал излагается последовательно и логично.

Оценка «4» - «хорошо» выставляется обучающемуся, если демонстрируются достаточно полное знание учебно-программного материала, не допускающий в ответе существенных неточностей, самостоятельно выполнивший все предусмотренные программой задания, усвоивший основную литературу, рекомендованную программой, активно работавший на практических занятиях, показавший систематический характер знаний по дисциплине, достаточный для дальнейшей учебы, а также способность к их самостоятельному пополнению.

Оценка «3» - «удовлетворительно» выставляется обучающемуся, если демонстрируются знания основного учебно-программного материала в объёме, необходимом для дальнейшей учебы и предстоящей работы по профессии, не отличавшийся активностью на практических занятиях, самостоятельно выполнивший основные предусмотренные программой задания, однако допустивший погрешности при их выполнении и в ответе на экзамене, но обладающий необходимыми знаниями для устранения под руководством преподавателя наиболее существенных погрешностей.

Оценка «2» - «неудовлетворительно» выставляется обучающемуся, если обнаруживаются пробелы в знаниях или отсутствие знаний по значительной части основного учебно-программного материала, не выполнившему самостоятельно предусмотренные программой основные задания, допустившему принципиальные ошибки в выполнении предусмотренных программой заданий, не отработавшему основные практические, семинарские, лабораторные занятия, допускающему существенные ошибки при ответе, и который не может продолжить обучение или приступить к профессиональной деятельности без дополнительных занятий по соответствующей дисциплине.