Приложение 1.1
к программе СПО
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ. 01. Эксплуатация информационно-телекоммуникационных систем и сетей

1.1. Цель и планируемые результаты освоения профессионального модуля

1.1.1. В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности: эксплуатация информационно-телекоммуникационных систем и сетей и соответствующие ему профессиональные и общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1.	**Эксплуатация информационно-телекоммуникационных систем и сетей**
ПК 1.1	Производить монтаж, настройку, проверку 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.

1.1.2. Перечень общих компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
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 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь Навыки	- монтажа, настройки, проверки функционирования и конфигурирования оборудования информационно-телекоммуникационных систем и сетей (ИТКС); - текущего контроля функционирования оборудования ИТКС; - проведения технического обслуживания, диагностики технического состояния, поиска неисправностей и ремонта 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 телекоммуникационных систем; - проводить работы по техническому обслуживанию, диагностики технического состояния и ремонту оборудования ИТКС; - измерять основные качественные показатели и характеристики при выполнении профилактических и ремонтных работ приемо-передающих устройств (ППУ); - читать принципиальные схемы блоков ППУ; - выполнять расчеты, связанные с определением значений параметров режима и элементов ППУ; - контролировать работу и осуществлять техническую эксплуатацию ППУ; - настраивать, эксплуатировать и обслуживать локальные вычислительные сети; - сопрягать между собой различные телекоммуникационные устройства; - производить настройку программного обеспечения коммутационного оборудования телекоммуникационных систем; - осуществлять настройку модемов, используемых в защищенных телекоммуникационных системах; - проверять функционирование, производить регулировку и контроль основных параметров источников питания радиоаппаратуры; - проводить типовые измерения; - пользоваться стандартными средствами электрорадиоизмерений; - оценивать точность проводимых измерений;

	- оформлять эксплуатационную и ремонтную документацию;
знать	- принципы построения информационно-телекоммуникационных систем и сетей; - базовые технологии построения и состав оборудования мультисервисных сетей связи; - состав и основные характеристики типового оборудования ИТКС; - принципы передачи информации в ИТКС; - принцип модуляции сигналов ИТКС; - принципы помехоустойчивого кодирования сигналов ИТКС; виды и характеристики сигналов в ИТКС; - принципы аналого-цифрового преобразования, работы компандера, кодера и декодера; особенности распространения электромагнитных волн различных диапазонов частот; - виды помех в каналах связи, методы защиты от них; разновидности проводных линий передачи; - конструкцию и характеристики электрических и оптических кабелей связи; - способы коммутации в сетях связи; - принципы построения многоканальных систем передачи; - принципы построения радиолиний и систем радиосвязи; - основы маршрутизации в информационно-телекоммуникационных сетях; - принципы построения, основные характеристики и оборудование систем подвижной радиосвязи; - технологии и оборудование удаленного доступа в информационно-телекоммуникационных сетях; - типовые услуги, предоставляемые с использованием информационно-телекоммуникационных сетей, виды информационного обслуживания, предоставляемые пользователям; - принципы построения и технические средства локальных сетей; - принципы функционирования маршрутизаторов; модемы, использующиеся в ИТКС, принципы подключения и функционирования; - спецификацию изделий, комплектующих, запасного имущества и ремонтных материалов, порядок их учета и хранения; - принципы организации эксплуатации ИТКС; - содержание технического обслуживания и восстановления работоспособности оборудования ИТКС; - принципы организации и технологию ремонта оборудования ИТКС; - периодичность поверок контрольно-измерительной аппаратуры; - принцип действия выпрямителей переменного тока; - принципы работы стабилизаторов напряжения и тока, импульсных

	источников питания. - принципы защиты электронных устройств от недопустимых режимов работы; - принципы построения, основные характеристики типовых измерительных приборов и правила работы с ними; - основные понятия и определения метрологии, стандартизации и сертификации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: 707 часов.
Из них на освоение МДК – 652 часов:

МДК.01.01Приемо-передающие устройства, линейные сооружения связи и источники электропитания- 160 часов;

в том числе самостоятельная работа 49 часов;

МДК.01.02Телекоммуникационные системы и сети - 284 часа;

в том числе самостоятельная работа 103 часа;

МДК.01.03Электрорадиоизмерения и метрология - 90 часов.

в том числе самостоятельная работа 18 часов;

На практики, в том числе учебная 108 часов

производственная -144 часа.

2. СТРУКТУРА и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе					
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация	Учебная	Производственная
1	*2*	*3*	*4*	*5*	*6*		*7*	*8*	*9*	*10*
ПК 1.1-1.4 ОК 1 –4, ОК 9,10	Раздел 1. Приемо-передающие устройства, линейные сооружения связи и источники электропитания	**160**		**160**	62		49			
ПК 1.1-1.4	Раздел 2. Телекоммуникационные системы и сети	**284**		**284**	88		103			
ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10	Раздел 3. Электрорадиоизмерения и метрология	**90**		**90**	36		36			
	Учебная практика	**108**							**108**	
	Производственная	**144**								**144**

	практика									
	Промежуточная аттестация	**27**								
	Всего:	***813***		***534***	***186***		***188***		***108***	***144***

2.2. Тематический план и содержание профессионального модуля (ПМ.01)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем часов	Код ПК, ОК
1	2	3	4
Раздел 1. Приемо-передающие устройства, линейные сооружения связи и источники электропитания		**160**	
МДК 01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания		**160**	
Подраздел 1. Технические средства и обслуживание передающего оборудования защищённых телекоммуникационных систем		**29**	
Тема 1.1. Назначение, структурная схема и технические характеристики радиопередатчика.	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Определение и назначение радиопередающего устройства (РПдУ). Обобщённая структурная схема передатчика и основные характеристики передатчика. Назначение основных каскадов РПдУ.		
Тема 1.2. Автогенераторы	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Условия самовозбуждения активных колебательных систем, баланс фаз, баланс амплитуд. Рабочая частота автогенератора **(**АГ). Схема транзисторного и лампового АГ. Режимы работы АГ. Принципы синхронизма и фазировки. Дестабилизирующие факторы и борьба с ними.		
Тема 1.3. Стабильность частоты автогенератора. Кварцевая стабилизация частоты. Кварцевые автогенератоы	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Стабильность частоты АГ, методы ее повышения. Кварцевая стабилизация частоты АГ. Устройство и работа кварцевого резонатора. Схемы включения кварцевого резонатора в АГ. Коррекция частоты кварцевого АГ. Преимущества и недостатки кварцевой стабилизации частоты. Схема кварцевого транзисторного АГ.		
Тема 1.4. Формирование сигналов.	**Содержание**	**1**	ПК 1.1-1.4

Возбудители и синтезаторы частот	Принципы формирования сигналов при различных методах синтеза частот. Понятие возбудителя - синтезатора частот, сетки и шага сетки частот. Методы синтеза частот. Автоматическая подстройка частоты (АПЧ) и её параметры. Частотная АПЧ. Фазовая АПЧ. Цифровой синтезатор частот.		ОК 1 –4, ОК 9,10
Тема 1.5. Режимы и принципы построения генераторов с внешним возбуждением. Схемы генераторов с внешним возбуждением (ГВВ)	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Обобщенная структурная схема и параметры ГВВ. Генераторы с внешним возбуждением: резонансные и широкополосные. Области применения резонансных и широкополосных ГВВ. Принцип работы и методика энергетического расчета ГВВ.		
Тема 1.6. Общие сведения о модуляции. Амплитудная модуляция сигналов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Общие сведения о различных видах модуляции и их особенностях. Понятия амплитудной модуляции (АМ), глубины модуляции и перемодуляции, спектр АМ колебания. Однополосная модуляция. Транзисторный амплитудный модулятор с коллекторной модуляцией. Области применения АМ.		
Тема 1.7. Частотная модуляция. Стабилизация частоты несущей при частотной модуляции	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Особенности угловых видов модуляции. Понятие частотной модуляции (ЧМ), девиации частоты, спектр ЧМ сигнала. Транзисторный частотный модулятор на основе варикапа. Стабилизация частоты несущей при частотной модуляции. Области применения ЧМ.		
Тема 1.8. Фазовая модуляция. Виды фазовых модуляторов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Понятие фазовой модуляции (ФМ), девиация фазы, спектр ФМ сигнала. Зависимость изменения угла фазы сигнала от амплитуды модулирующего колебания. Схемы построения фазовых модуляторов.		
Тема 1.9. Импульсная модуляция. Схемы импульсных модуляторов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Понятие импульсной модуляции (ИМ). Виды ИМ и её особенности. Структурная схема передатчика с ИМ. Параметры и спектр сигнала при ИМ. Структурная схемы модуляторов ИМ. Внутриимпульсная частотная		

	модуляция.		
	Практические занятия	**16**	
	Исследование влияния дестабилизирующих факторов на работу автогенератора	2	
	Исследование генератора, управляемого напряжением, используемого в синтезаторах частот	4	
	Исследование умножителя частоты	2	
	Исследование амплитудного модулятора	4	
	Исследование частотного модулятора	4	
Подраздел 2. Техническое обслуживание и оборудование приемных устройств телекоммуникационных систем		**28**	
Тема 2.1. Теоретические основы радиоприема. Структурные схемы радиотрактов приёмников. Основные понятия и характеристики радиоприёмных устройств	**Содержание**		ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение, основные характеристики радиоприемных устройств (РПмУ). Структурная схема РПмУпрямого усиления. Структурная схема супергетеродинногоРПмУ и её особенности.	**1**	
Тема 2.2. Входные цепи приёмных устройств. Особенности входных цепей различных частотных диапазонов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение входной цепи, классификация и основные характеристики. Структура входной цепи (ВЦ). ВЦ с сосредоточенными и распределенными элементами. Методика электрического расчета ВЦ.		
Тема 2.3. Резонансные усилители. Усилители радиочастоты. Малошумящие усилители СВЧ.	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение и основные характеристикирезонансного усилителя. Структурная схема резонансного усилителя и режимы его работы. Малошумящие усилители сверхвысоко частоты (СВЧ). Методика электрического расчета усилителя СВЧ.		
Тема 2.4. Преобразователи частоты радиоприемников. Виды	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4,
	Назначение, структура и принцип работы преобразователя частоты (ПЧ). ПЧ		

преобразователей частоты	с отдельным гетеродином. ПЧ с совмещённым гетеродином. Расчёт промежуточной частоты и преобразователя частоты.		ОК 9,10
Тема 2.5. Усилители промежуточной частоты радиоприемных устройств	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение и схемотехника усилителя промежуточной частоты (УПЧ). Стандартные промежуточные частоты радиоприёмных устройств. Многокаскадные УПЧ. Избирательные элементы в УПЧ.		
Тема 2.6. Детекторы сигналов. Амплитудное детектирование. Детекторы импульсных сигналов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Процесс детектирования сигналов. Амплитудные детекторы и их основные характеристики. Нелинейные и инерционные искажения в амплитудных детекторах. Импульсное детектирование сигналов.		
Тема 2.7. Амплитудные ограничители. Принцип работы частотных детекторов. Виды частотных детекторов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Амплитудные ограничители. Назначение, основные характеристики и принцип работы частотного детектора. Схемотехника частотных детекторов.		
Тема 2.8. Принцип работыфазовых детекторов. Виды фазовых детекторов	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение, принцип работы и основные характеристики фазового детектора (ФД).Искажения характеристики ФД. СхемотехникаФД.		
Тема 2.9. Регулировки в радиоприёмных устройствах	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Регулировка усиления. Настройки радиоприемников. Регулировка полосы пропускания. Устройства индикации РПМУ.		
Тема 2.10. Автоматическая регулировка усиления	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение, параметры и принцип работы схем автоматической регулировки усиления (АРУ). Основные схемы АРУ.		
Тема 2.11. Автоподстройка частоты в радиоприёмных устройствах	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Принцип автоматической подстройки частоты в радиоприемных устройствах. Структурные схемы систем АПЧ различных видов, назначение каскадов. Основные характеристики системы АПЧ.		
Тема 2.12. Регулировка полосы пропускания	**Содержание**	**1**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Способы регулировки полосы пропускания приёмника Особенности регулировок полосы пропускания в различных каскадах радиоприёмника.		

	Практические занятия	**16**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Исследование резонансного усилителя радиочастоты	2	
	Исследование преобразователя частоты с отдельным гетеродином	4	
	Исследование усилителя промежуточной частоты	2	
	Исследование отдельных функциональных блоков систем радиосвязи	4	
	Исследование отдельных функциональных блоков систем радиосвязи	4	
Подраздел 3. Линии связи		**47**	
Тема 3.1. Построение сетей электросвязи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Виды направляющих систем и их основные свойства. Системы многоканальной передачи по линиям связи. Основные требования к линиям связи. Построение линейных сооружений сетей электросвязи. Построение магистральных сетей связи. Построение зоновых сетей связи. Построение местных сетей связи.		
Тема 3.2. Воздушные линии связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Конструктивные элементы воздушных линий связи (ВЛС). Назначение, состав и основные параметры ВЛС. Проволока, изоляторы, крюки, штыри, траверсы, опоры.		
Тема 3.3. Кабельные линии связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Классификация, конструкция, характеристики и маркировка электрических кабелей связи. Конструктивные элементы кабелей: токопроводящие жилы, изоляция жил, скрутка в группы, кабельный сердечник, поясная изоляция, экран, оболочка, внешние защитные покровы.		
Тема 3.4. Кабели телефонных сетей и сетей проводного вещания	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Кабели телефонных сетей и сетей проводного вещания (ПВ). Конструкция и назначение кабелей ТПП; кабелей с витой парой UTP, STP; кабелей для соединительных линий и кабельных вставок типа ТЗ; кабелей межстанционных сетей (сельских) КСП, однопарных кабелей СТС и ПВ		

	марок ПРППМ, МРМ, ПТПЖ, ТРП (ТРВ); станционных кабелей ТСВ.		
	Практические занятия	**6**	
	Кабели ПВ	2	
	Кабели ТПП	2	
	Кабели СТС	2	
Тема 3.5. Кабели магистральных и зоновых сетей	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Конструкция симметричных кабелей типов МКС, ЗК. коаксиальных кабелей МКТ-4, КМ-4,-75, КРК-75.		
	Практические занятия	**4**	
	Симметричные кабели	2	
	Коаксиальные кабели	2	
Тема 3.6. Волоконно-оптические линии связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Основы передачи информации по волоконно-оптическим линиям связи (ВОЛС). Структура и компоненты линейного тракта ВОЛС. Характеристики оптических компонентов ВОЛС.		
	Практические занятия	**2**	
	Волоконно-оптические линии связи	2	
Тема 3.7. Кабельная Подземная инфраструктура телефонной связи	**Содержание**	**3**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Назначение, состав и требования к подземной инфраструктуре телефонной связи. Строительство кабельной канализации, применение средств механизации. Прокладка кабеля в телефонной канализации. Особенности прокладки кабелей ВОЛС.		
Тема 3.8. Прокладка кабельных линий	**Содержание**	**2**	ПК 1.1-1.4

связи	Подготовка кабеля к прокладке и электрические измерения. Согласование и разбивка трассы. Механизированная и ручная прокладка кабелей. Прокладка оптических кабелей. Особенности прокладки кабелей через водные преграды и на пересечении с построенными сооружениями		ОК 1 –4, ОК 9,10
Тема 3.9. Монтаж кабелей связи и оконечных кабельных устройств местных телефонных сетей	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Организация монтажных работ. Монтажные инструменты, приспособления, материалы. Проверка кабелей перед монтажом. Требования к монтажу. Принципы разделки концов кабелей для прямого соединения. Измерения смонтированных участков. Назначение, конструкция, маркировка и места установки оконечных кабельных устройств (ОКУ) и их монтаж.		
	Практические занятия	**12**	
	Монтаж кабеля ТПП, МКС, ЗКП	4	
	Монтаж КРТП-10, БМ	4	
	Монтаж МТОК	4	
Тема 3.10. Устройства ввода кабелей в здания станций (УП, ОУП), телефонизируемые здания	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Кроссирование кабелей в АТС. Назначение шахты. Кроссирование кабелей в абонентские пункты.		
Тема 3.11. Кабели под постоянным воздушным избыточным давлением	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Эксплуатация кабелей под постоянным избыточным воздушным давлением. Системы и установки для эксплуатации кабелей давлением. Методы определения района и места повреждения оболочки кабеля		
Подраздел 4. Электрические характеристики направляющих систем передачи		**4**	
Тема 4.1. Электрические характеристики воздушных и кабельных линий связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Первичные и вторичные параметры электрических кабелей и воздушных линий связи (ВЛС). Частотные диапазоны использования электрических кабелей и ВЛС		
Тема 4.2. Параметры волоконно-	**Содержание**	**2**	ПК 1.1-1.4

оптических линий	Параметры волоконно-оптических линий (ВОЛС). Критическая частота и длина волн волоконного световода. Типы волн в световоде. Затухание волоконных световодов. Дисперсия и пропускная способность световодов.		ОК 1 –4, ОК 9,10
	Практические занятия	**2**	
	Измерение электрических характеристик симметричных кабелей	2	
Подраздел 5. Взаимные влияния в линиях связи и меры по их уменьшению		**6**	
Тема 5.1. Взаимные влияния между цепями воздушных и кабельных линия связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Взаимное влияние в оптических кабелях. Причины взаимных влияний между цепями воздушных и кабельных линия связи. Параметры влияния. Причины взаимных влияний между оптическими волокнами		
Тема 5.2. Обеспечение электромагнитной совместимости линий связи и проводного вещания	**Содержание**	**4**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Способы защиты от взаимных влияний. Способы уменьшения взаимных влияний на кабельных НЧ и ВЧ линиях. Измерительные приборы, применяемые при симметрировании. Защита световодных трактов от взаимных помех. Приобретение навыков тестирования смонтированных устройств в кабельных линиях связи.		
Раздел 6. Защита линий связи от влияния внешних источников и коррозии		**8**	
Тема 6.1. Источники опасных и мешающих влияний. Меры защиты линейных сооружений связи	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Основные понятия об источниках электромагнитного влияния на линии связи. Меры защиты линейных сооружений от опасного влияния атмосферного электричества, линий электропередачи, электрифицированного транспорта и радиостанций. Схемы защиты и элементы защиты. Оборудование заземлений.		
Тема 6.2. Защита сооружений связи от коррозии	**Содержание**	**2**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Основные виды коррозии: почвенная, атмосферная, электролитическая, межкристаллитная. Их характеристика. Меры защиты от коррозии.		
	Практические занятия	**4**	
	Исследование элементов защиты от внешних влияний	2	
	Измерения при защите кабеля от коррозии	2	

Подраздел 7. Техническое обслуживание линий связи		**4**	
Тема 7.1. Организация и осуществление технической эксплуатации линейных сооружений местных телефонных сетей	**Содержание**	**4**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Организация эксплуатации. Задачи и методы технической эксплуатации. Охрана кабельных сооружений и аварийно-восстановительные работы. Электрические измерения в процессе эксплуатации.		
Тема 7.2. Надежность линий связи	**Содержание**	**4**	ПК 1.1-1.4 ОК 1 –4, ОК 9,10
	Обеспечение надежности линий связи. Показателинадежности. Оценка надежности и мероприятия по повышению надежности на линиях связи.		
Самостоятельная работа при изучении раздела ПМ		**49**	
Рекомендуемая примерная тематика внеаудиторной самостоятельной работы для разработчиков программ образовательной организации: 1. Обобщённая структурная схема передатчика. Назначение основных каскадов передатчика. 2. Схема транзисторного и лампового автогенератора. Режимы работы АГ. 3. Частотная АПЧ. Фазовая АПЧ. Цифровой синтезатор частот. 4. Принцип работы и методика энергетического расчета ГВВ. 5. Транзисторный амплитудный модулятор с коллекторной модуляцией. Транзисторный частотный модулятор на основе варикапа. Схемы построения фазовых модуляторов. 6. Структурная схемы импульсных модуляторов. 7. Методика электрического расчета ВЦ, усилителя СВЧ, УПЧ. 8. Построение линейных сооружений сетей электросвязи. Назначение, состав и основные параметры ВЛС. 9. Конструктивные элементы кабелей. Кабели телефонных сетей и сетей проводного вещания. 10. Конструкция и назначение кабелей ТПП. Структура и компоненты линейного тракта ВОЛС. 11. Прокладка оптических кабелей. Назначение, конструкция, маркировка и места установки ОКУ и их монтаж. 12. Первичные и вторичные параметры электрических кабелей и ВЛС. 13. Защита ВЛС и трактов от взаимных помех. 14. Схемы и элементы защиты линейных сооружений. Оборудование заземлений.			ПК 1.1-1.4 ОК 1 –4, ОК 9,10
Всего		**160**	
Раздел 2. Телекоммуникационные системы и сети		**284**	
МДК.01.02. Телекоммуникационные системы и сети		**284**	

Подраздел 1. Построение телекоммуникационных систем и сетей		**44**	
Тема 1.1. Основы построения сетей связи	**Содержание**	**2**	ПК 1.1-1.4
	Единая Сеть Электросвязи Российской Федерации (ЕСЭ РФ). Состав и назначение ЕСЭ РФ. Архитектура сетей. Первичные и вторичные сети, службы связи. Абонентское оборудование. Структура телекоммуникационных сетей. Системы передачи и коммутации информации. Классификация телекоммуникационных сетей.		
Тема 1.2. Эталонная модель взаимодействия открытых систем	**Содержание**	**3**	ПК 1.1-1.4
	Стандартизация в телекоммуникациях. Открытые системы в телекоммуникациях. Эталонная модель взаимодействия открытых систем (ЭМВОС). Иерархия взаимодействия открытых систем. Единицы данных уровней ЭМВОС. Функции уровней ЭМВОС. Инкапсуляция данных в ЭМВОС.		
Тема 1.3. Системы коммутации в телекоммуникационных сетях	**Содержание**	**3**	ПК 1.1-1.4
	Виды коммутации в телекоммуникационных сетях. Коммутация каналов. Коммутация пакетов. Технологии коммутации пакетов. Модель пакетного коммутатора. Датаграммная передача. Виртуальные каналы. Логическое соединение.		
	Практические занятия	**4**	
	Изучение принципов частотного разделения каналов (ЧРК). Построение и система нумерации в телефонной сети связи.		
Тема 1.4. Системы сигнализации	**Содержание**	**4**	ПК 1.1-1.4
	Сигнализация в телефонных сетях. Сигналы сигнализации. Виды сигнализации. Сигнализация по выделенному каналу (ВСК-2). Общеканальная сигнализация (ОКС-7).		
Тема 1.5. Цифровые системы передачи	**Содержание**	**2**	ПК 1.1-1.4
	Принцип временного разделения каналов (ВРК). Цифровые системы передачи с ВРК. Теорема Котельникова. Расчет частоты дискретизации. Импульсные виды модуляции. Методика расчета структуры временного цикла. Цифровые системы передачи с импульсно-кодовой модуляцией		

	(ИКМ). ИКМ-30/32. Каналы Е1, Е2, Е3, Е4.		
	Практические занятия	**4**	
	Исследования спектра сигналов с импульсной модуляцией	2	
	Исследование принципа работы канала с ВРК	2	
Тема 1.7. Кодирующие и декодирующие устройства цифровых систем передачи	**Содержание**	**2**	ПК 1.1-1.4
	Назначение и классификация кодеров. Область применения нелинейных кодеров взвешивающего типа. Структурная схема кодирующих устройств. Назначение узлов. Этапы нелинейного кодирования. Достоинства и недостатки нелинейных кодеров. Назначение декодеров. Область применения нелинейных декодеров взвешивающего типа. Структурная схема декодирующих устройств. Назначение узлов. Этапы нелинейного декодирования. Достоинства и недостатки нелинейных декодеров.		
	Практические занятия	**6**	
	Нелинейные кодеры взвешивающего типа	4	
	Нелинейные декодеры взвешивающего типа	2	
Тема 1.8. Формирование управляющих сигналов в генераторном оборудовании цифровых систем передачи	**Содержание учебного материала**	**2**	ПК 1.1-1.4
	Структурная схема и принципы построения генераторного оборудования (ГО). Назначение узлов ГО, Требования к задающему генератору. Отличие ГО передачи от ГО приема.		
	Практические занятия	**2**	
	Расчет частот ГО цифровой системы передачи		
Тема1.9. Синхронизация в цифровых системах передачи	**Содержание**	**2**	ПК 1.1-1.4
	Назначение и виды синхронизации. Требования к системам синхронизации. Обобщенные схемы УТС, ПЦС.		
	Практические занятия	**4**	
	Приемник сигналов цикловой синхронизации	4	
Тема 1.10. Формирование линейных цифровых сигналов в системах передачи	**Содержание**	**2**	ПК 1.1-1.4
	Требования к линейным кодам. Алгоритмы формирования, достоинства и недостатки линейных кодов. Принцип работы преобразователя кода передачи и преобразователя кода приема.		

	Практические занятия	**6**	
	Преобразователь кода передачи	2	
	Преобразователь кода приема	2	
	Формирование линейных кодов в цифровых системах передачи	2	
Тема 1.11. Регенерация цифрового сигнала в системах передачи	**Содержание**	**2**	ПК 1.1-1.4
	Назначение, классификация, структурные схемы, параметры регенераторов. Устройства тактовой синхронизации в регенераторах. Оценка качества работы регенераторов.		
Подраздел 2. Системы радиосвязи		**6**	
Тема 2.1. Радиорелейные и спутниковые системы связи	**Содержание**	**1**	ПК 1.1-1.4
	Распространение радиоволн. Виды радиоволн. Особенности распространения волн различных диапазонов. Антенно-фидерные устройства. Передающие антенны. Приемные антенны. Фидеры. Принцип радиорелейной связи. Построение цифровых радиорелейных линий связи (ЦРРЛ). Цифровая радиорелейная станция. Спутниковые системы связи (ССС). Построение ССС. Земные станции ССС.		
Тема 2.2. Системы сотовой подвижной радиосвязи	**Содержание**	**1**	ПК 1.1-1.4
	Эволюция сетей подвижной связи (СПС). Сетевая технология GSM. Подсистема базовой станции, регистры HLR и VLR, центр коммутации подвижной связи, центр аутентификации и регистр идентификации оборудования. Системы сигнализации СПС. Технологии и услуги сетей UMTS. Сети стандартов 3G, 4G, LTE.		
	Практические занятия	**4**	
	Расчет основных параметров сетей подвижной связи	4	
Подраздел 3. Монтаж и эксплуатация телекоммуникационных систем и сетей		**88**	
Тема 3.1. Монтаж, настройка и эксплуатация оборудования цифровых систем передачи	**Содержание**	**8**	ПК 1.1-1.4
	Технологии систем плезиохронной цифровой иерархии**.** Структура систем передачи Е1. Основные характеристики интерфейса Е1. Виды линейных кодов. Цикловая и сверхцикловая структура Е1. Процедуры контроля ошибок		

	передачи CRC-4. Сетевой уровень Е1. Технологии мультиплексирования цифровых потоков. Принцип и способы мультиплексирования. Синхронное мультиплексирование. Мультиплексирование асинхронных потоков. Система команд согласования скоростей. Параметры каналов ТЧ. Нормирование и методика измерений. Канал ТЧ, оценка качества каналов, методика измерений параметров. Виды измерительных приборов и осуществление измерения параметров. Анализ результатов измерений. Особенности построения первичных мультиплексоров. Оборудование ОГМ-30. Назначение, основные технические данные, функциональные схемы основных узлов. Структура временного цикла. Программное обеспечение ОГМ-30. Назначение КПО-110. Оборудование МП СуперТел. Назначение, основные технические данные, состав оборудования. Структурные схемы основных узлов оборудования. Структура временного цикла. Программное обеспечение «СуперТел». Нормирование параметров ОЦК и групповых цифровых трактов. ОЦК и групповые цифровые тракты. Нормирование параметров. Выбор измерительных приборов. Методика измерений параметров цифровых каналов и трактов. Анализ результатов измерений.		
	Практические занятия	**22**	
	Измерение параметров каналов ТЧ анализатором телефонных каналов AnComTDA-5	4	
	Разработка проектов с помощью КПО-110 на МП ОГМ-30	4	
	Организация локального и удаленного доступа в МП «Супертел»	4	
	Измерение параметров групповых цифровых трактов прибором ТИС-Е1	4	
	Мультиплексирование цифровых потоков	2	
	Расчет основных параметров цифровых систем передачи	4	
Тема 3.2. Монтаж, первичная	**Содержание**	**4**	ПК 1.1-1.4

инсталляция, мониторинг оборудования проводного цифрового доступа	ТехнологияхDSL.Технологии кодирования, применяемые в xDSL.Технология HDSL.Типовые параметры и разновидности оборудования HDSL. Область применения оборудования HDSL. Оборудование FlexDSLPAME1. Назначение, технические данные, основы применения. Оборудование FlexDSLORION-2.Назначение, технические данные, область применения. Мониторинг и конфигурирование FlexDSLORION-2. Анализ результатов мониторинга.		
	Практические занятия	**8**	
	Мониторинг оборудования FlexDSLPAME1	4	
	Организация локального и удаленного конфигурирования оборудования FlexDSLOrion-2	4	
	Формирование линейных кодов абонентских линий	4	
Тема 3.3. Инсталляция, настройка и эксплуатация оборудования волоконно-оптических систем передачи на базе технологии SDH	**Содержание**	**10**	ПК 1.1-1.4
	Волоконно-оптических системы передачи (ВОСП). Пассивные и активные компоненты ВОСП. Принцип построения ВОСП. Линейные коды ВОСП. Построение цифровых систем SDH. Синхронные цифровые телекоммуникационные системы. Основные информационные структуры. Формирование модуля STM-1. Мультиплексирование STM-N. Структуры кадров СЦТС. Виды мультиплексоров SDH. Топология, архитектура, синхронизация сетей. Резервирование трактов. Семейство оборудования SDH «Alcatel-Lucent». Технические данные, назначение, область применения. Возможности программного обеспечения. Мультиплексор WaveStar AMI+. Технические данные, назначение, область применения, состав оборудования. ПО. Назначение информационных и аварийных сигналов. Просмотр и анализ аварийных сообщений. Алгоритм поиска и устранения неисправностей. Оборудование SDH «Alcatel 1664SM», «Alcatel 1655/1666SR». Технические данные, назначение, область применения, состав оборудования. Назначение информационных и аварийных сигналов. Просмотр и анализ аварийных		

	сообщений. Алгоритм поиска и устранения неисправностей.		
	Практические занятия	**20**	
	Конфигурирование мультиплексора WaveStar AMI+	4	
	Конфигурирование источников синхронизации сетевого элемента мультиплексора WaveStar AMI+	4	
	Конфигурирование и резервирование трактов мультиплексора WaveStar AMI+	4	
	Анализ систем SDH при помощи анализатора NGSDH «VictoriaCombo»	4	
	Формирование линейных кодов ВОСП	4	
	Формирование модулей STM-N	4	
Тема 3.4. Инсталляция, настройка и эксплуатация оборудования ВОСП технологии WDM	**Содержание**	**8**	ПК 1.1-1.4
	Технология оптического мультиплексирования WDM. Достоинства и недостатки технологии WDM**.** Классификация WDM-систем.Канально-частотный план. Структурная схема системы передачи с WDM**.** Семейство оборудования HuaweiOptixMetro.Разновидности оборудования**,** назначение, технические данные, состав оборудования, область применения. Инсталляция, конфигурирование и мониторинг оборудования. Виды и		

	назначение информационных и аварийных сигналов. Просмотр и анализ аварийных сообщений. Алгоритм поиска и устранения неисправностей.		
	Практические занятия	**8**	
	Изучение оборудования «Huawei Optix Metro 6040»	4	
	Организация локального и удаленного конфигурирования оборудования «HuaweiOptixMetro 6040»	4	
Самостоятельная работа при изучении раздела ПМ		**103**	
Рекомендуемая тематика внеаудиторной самостоятельной работы: 1. Состав и назначение ЕСЭ РФ. Архитектура сетей. Первичные и вторичные сети, службы связи. Функции уровней ЭМВОС. 2. Технологии коммутации пакетов. 3. Цифровые системы передачи с импульсно-кодовой модуляцией (ИКМ). ИКМ-30/32. Каналы Е1, Е2, Е3, Е4. 4. Устройства тактовой синхронизации в регенераторах ЦСП ИКМ. 5. Спутниковые системы связи. Земные станции ССС. 6. Сети стандартов 3G, 4G, LTE. 7. Типовые параметры и разновидности оборудования HDSL 8. Виды мультиплексоров SDH. Топология, архитектура, синхронизация сетей. 9. Структурная схема системы передачи с WDM. 10. Решение задачи на расчет частоты дискретизации 11. Решение задач на нелинейное кодирование и декодирование ЦСП 12. Решение задач на расчет управляющих частот генераторного оборудования ЦСП 13. Решение задач на построение линейных кодов ЦСП и ВОСП 14. Составить таблицу анализа параметров источников и приемников оптического излучения 15. Составить схему организации связи ЦСП и ВОСП местной сети, внутризоновой и магистральной сети 16. Составить таблицу технических характеристик и состава оборудования ЦСП и ВОСП местной, внутризоновой, магистральной сетей 17. Подготовить презентацию по ВОСП местных, внутризоновых и магистральных сетей			ПК 1.1-1.4

18. Составить паспорта на каналы, сетевые тракты и на аппаратуру систем передачи 19. Составить схемы измерений параметров каналов 20. Составить таблицы стандартов и протоколов информационных сигналов, норм ошибок в каналах и трактах,видов аварийных сигналов и аварийной сигнализации.			
Примерная тематика домашних заданий: 1.Систематическое изучение конспектов занятий, выполнение заданий в рабочих тетрадях. 2.Изучение учебной и специальной технической литературы. 3.Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателей. 4.Оформление отчетов по лабораторно-практическим работам. 5.Осуществление поиска необходимой информации в различных источниках. 6.Использование в подготовке к выполнению лабораторных и практических работ проектной и технической документации. 7.Разработка рефератов по современным технологиям в телекоммуникациях.			ПК 1.1-1.4
Всего		**284**	
Раздел 3. Электрорадиоизмерения и метрология		**90**	
МДК.01.03. Электрорадиоизмерения и метрология		**90**	
Введение	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Ключевые понятия дисциплины. Предмет и задачи дисциплины, структура дисциплины. Профессиональная значимость дисциплины, межпредметные связи с другими дисциплинами. Правовые основы метрологии, стандартизации и подтверждения соответствия. Краткие исторические сведения развития измерений, стандартизации.		
Подраздел 1. Основы метрологии		**26**	
Тема 1.1. Наука об измерении, физические величины	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения о метрологии, стандартизации и сертификации. Метрология как наука об измерениях.		
Тема 1.2. Измерение физических величин	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения об измерении электрического сигнала. Физические величины, шкалы, системы физических величин. Измерение физических величин, суть простейшего измерения. Классификация измерений,		

	характеристики качества измерения.		
Тема 1.3. Средства измерений	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения о средствах измерения, классификация средств измерения. Элементарные средства измерения. Комплексные средства измерения. Характеристики средств измерения. Эталоны основных физических единиц.		
Тема 1.4. Методы измерений	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения о теории измерений. Физические явления и эффекты, положенные в основу измерений. Методы измерений. Методика выполнения измерения.		
	Практические работы	**12**	
	Физические величины и их единицы	4	
	Технические средства для измерений	4	
	Измерение физической величины	4	
Тема 1.5. Основы теории погрешностей измерений	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения. Классификация погрешностей. Систематические погрешности. Случайные погрешности. Классы точности средств измерения.		
Тема 1.6. Обработка результатов измерений	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Цель и задачи обработки результата измерений. Способы выражения результатов измерений, запись результатов измерений. Формы предоставления результатов измерений. Правила округления результатов измерений. Номинальные значения влияющих величин при нормальных условиях. Обработка и оценка результатов измерений.		
Тема 1.7. Государственная система обеспечения единства измерений	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Цель и задачи государственной системы обеспечения единства измерений (ГСОЕИ). Законодательная база ГСОЕИ. Нормативная база ГСОЕИ. Метрологический надзор.		
Подраздел 2. Измерительные приборы		**10**	
Тема 2.1. Принципы построения средств измерения	**Содержание**	**2**	ПК 1.1, 1.2, 1.4
	Обобщённая структурная схема измерительного прибора. Шкалы		

	измерительных приборов, цена деления шкалы прибора.		ОК 1 –4, ОК 9, 10
Тема 2.2. Аналоговые измерительные приборы	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Аналоговые измерительные электромеханические приборы, буквенно-цифровое обозначение. Обобщённая структурная схема электромеханического прибора. Классификация аналоговых электромеханических приборов. Устройство и работа магнитоэлектрического измерительного механизма.		
Тема 2.3. Цифровые измерительные приборы	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения о цифровых приборах. Преобразование информации в цифровых устройствах. Коды, применяемые в цифровых приборах. Структурная схема цифрового измерительного прибора. Методы преобразования в аналого-цифровом преобразователе. Режимы работы цифрового прибора, элементы цифрового прибора.		
	Лабораторные работы	**4**	
	Аналоговые и цифровые измерительные приборы	2	
	Измерение электрического сигнала аналоговыми и цифровыми приборами	2	
Подраздел 3. Источники электрических сигналов		**6**	
Тема 3.1. Измерительные генераторы	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Назначение генераторов измерительных сигналов. Классификация генераторов. Схемы задающих генераторов. Установка частоты задающих генераторов.		
Тема 3.2. Основные типы генераторов сигналов	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Генераторы гармонических колебаний. Цифровые измерительные генераторы низких частот. Генераторы шумовых сигналов, импульсные генераторы. Стандарт частоты, синтезаторы частоты. Органы управления генератором, выходные цепи генераторов.		
	Лабораторные работы	**2**	
	Изучение работы генератора сигналов	1	
	Изучение работы генератора стандартных сигналов	1	

Подраздел 4. Методы и средства измерения параметров сигналов		**18**	
Тема 4.1. Измерение параметров тока, напряжения и мощности сигналов	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Измерение силы постоянного тока, расширение пределов измерения тока. Измерение переменного тока. Измерение напряжения электромеханическими приборами. Расширение пределов измерения напряжения. Выпрямительный прибор, термоэлектрический прибор. Классификация методов измерения мощности. Измерение мощности методом вольтметра или амперметра. Цифровые ваттметры.		
Тема 4.2. Измерение амплитудных и временных параметров сигналов	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Назначение осциллографа, классификация осциллографов. Структурная схема универсального осциллографа. Принцип получения изображения на экране осциллографа. Измерение амплитудных и временных параметров сигнала. Назначение органов управления осциллографом. Виды и назначение развёрток. Особенности применения различных осциллографов.		
Тема 4.3. Измерение информационных параметров сигналов	**Содержание**	**2**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Приборы для частотно-временных измерений. Измерение частоты и интервалов времени. Методы измерения фазового сдвига. Методы измерения амплитудно-модулированных сигналов. Цифровой измеритель параметров модулированных сигналов. Анализатор спектра последовательного типа. Измерение напряжённости электромагнитного поля.		
	Лабораторные работы	**12**	
	Измерение силы тока	1	
	Измерение напряжения	1	
	Измерение мощности	1	
	Изучение работы электронного осциллографа	1	
	Измерение параметров электрического сигнала с помощью электронного осциллографа	2	
	Измерение частоты и временного периода цифровым частотомером и электронным осциллографом	2	

	Измерение фазового сдвига	2	
	Измерение коэффициента амплитудной модуляции	2	
Подраздел 5. Методы и средства измерения параметров компонентов радиотехнических цепей		**8**	
Тема 5.1. Методы и средства измерения параметров компонентов радиотехнических цепей	**Содержание**	**4**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения, классификация методов измерения параметров. Измерение активных сопротивлений. Резонансные методы измерения параметров цепей. Цифровые приборы для измерения параметров элементов. Методы измерения параметров АЧХ. Структурная схема автоматического измерителя АЧХ. Методы измерения искажений формы сигнала. Цифровой измеритель нелинейных искажений формы сигнала.	1	
	Лабораторные работы	**4**	
	Измерение электрического сопротивления	1	
	Изучение работы измерителя иммитанса	1	
	Измерение амплитудно-частотных характеристик	1	
	Измерение нелинейных искажений	1	
Подраздел 6. Измерения в телекоммуникационных системах		**4**	
Тема 6.1. Измерения в телекоммуникационных системах	**Содержание**	**1**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения о средствах измерения для оценки защищенности конфиденциальной информации. Средства измерений в телекоммуникациях. Регламентные и эксплуатационные измерения. Современные измерительные средства.		
Тема 6.2. Средства защиты конфиденциальной информации	**Содержание**	**1**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Структурная схема генератора шумовых сигналов. Структурная схема измерителя шума и вибраций. Структурная схема измерителя уровня. Цифровой вольтметр.		
	Лабораторные работы	**2**	
	Изучение средств измерений для оценки защищённости конфиденциальной информации	1	
	Изучение работы цифрового вольтметра и цифрового измерителя уровня	1	

Подраздел 7. Основы технического регулирования		**3**	
Тема 7.1. Технические регламенты и стандарты	**Содержание**	**1**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения. Закон РФ «О техническом регулировании». Технические регламенты.	1	
Тема 7.2. Технические регламенты и стандарты	**Содержание**	**1**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Общие сведения. Сущность стандартизации. Цели стандартизации. Принципы стандартизации. Документы в области стандартизации.	1	
Тема 7.3. Сертификация продукции	**Содержание**	**1**	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
	Подтверждение соответствия и сертификация. Принципы и формы подтверждения соответствия. Добровольная сертификация. Обязательная сертификация.	1	
Самостоятельная работа при изучении раздела ПМ		**18**	
Рекомендуемая тематика внеаудиторной самостоятельной работы: 1. Характеристики средств измерения. Эталоны основных физических единиц. 2. Классы точности средств измерения. 3. Обобщённая структурная схема электромеханического прибора. 4. Структурная схема цифрового измерительного прибора. 5. Генераторы шумовых сигналов, импульсные генераторы. 6. Стандарт частоты, синтезаторы частоты. 7. Структурная схема автоматического измерителя АЧХ. 8. Цифровой измеритель нелинейных искажений формы сигнала. 9. Структурная схема генератора шумовых сигналов. 10. Структурная схема измерителя шума и вибраций. 11. Структурная схема измерителя уровня. 12. Цифровой вольтметр. 13.Добровольная и обязательная сертификация		18	ПК 1.1, 1.2, 1.4 ОК 1 –4, ОК 9, 10
Всего		**90**	
Учебная практика (по профилю специальности) итоговая по ПМ		**108**	

Виды работ Монтаж кабелей НЧ и ВЧ различными технологиями. Монтаж оконечных устройств, применяемых на местных телефонных сетях, магистральных и зоновых линиях связи для электрических и оптических кабелей. Контроль качества монтажа с применением измерительных приборов постоянного тока. Определение вида и места повреждения кабельной линии связи с помощью приборов переменного тока (рефлектометров). Монтаж оптических кабелей. Проверка качества монтажа оптических волокон с помощью рефлектометров и измерителей оптической мощности. Разделка кабелей с «витой парой» для включения в коннекторы соответствующей емкости. Монтаж коммутационных панелей. Испытание смонтированной линии тестерами. Оформление документации при сдаче линии в эксплуатацию.		
Производственная практика (по профилю специальности) итоговая по ПМ **Виды работ** Ознакомление со структурой предприятия, вводный инструктаж по технике безопасности и охране труда. Ознакомление с кабельными цехами и участками. Работа с технической документацией. Изучение оборудования и устройств, повышающих работоспособность и надежность кабельных линий. Ознакомление с оборудованием ИТКС. Изучение и работа с контрольно-измерительным оборудованием. Самостоятельная работа на закрепленном рабочем месте. Выполнение индивидуального задания по практике. Участите в аварийных и профилактических работах, проводимых на кабельном участке. Обобщение материала, оформление отчета, сдача зачета.	**144**	
Промежуточная аттестация	**27**	
Всего по ПМ	**813**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы предполагает наличие учебного кабинета, лаборатории.

Лаборатория «Информационно-телекоммуникационных систем и сетей», должна быть оснащена рабочими местами на базе вычислительной техники; стендами глобальных, локальных проводных и беспроводных сетей, сети сотовой связи, волоконно-оптической системы передачи с волновым и временным уплотнением каналов; комплектами структурированных кабельных (медножильной, волоконно-оптической) систем; комплектами устройств генерирования и формирования сигналов, устройств приема и обработки сигналов, входных и выходных цепей, устройств СВЧ и антенн; эмулятором (эмуляторами) активного сетевого оборудования; программным обеспечением сетевого оборудования;

- рабочие места для проведения исследования устройств электропитания;
- аппаратные или программно-аппаратные контрольно-измерительные приборы;
- макеты и/или устройства электропитания;
- цифровые и волоконно-оптические системы передачи;
- мультиплексоры;
- направляющие системы электросвязи на электрических и оптических кабелях;
- телекоммуникационные системы коммутации;
- оптический микроскоп, анализатор, оптические тестеры и рефлектометры;
- набор инструментов для выполнения кроссировочных работ;
- комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. К.Е. Самуйлов, И.А. Шалимов, Н.Н. Васин, В.В. Василевский, Д.С. Кулябов, А.В. Королькова Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов /. – М.: Издательство Юрайт, 2019. – 363 с.
2. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2019. – 944 с.
3. Томаси У. Электронные системы связи.- М.: Техносфера, 2020. -1360с.
4. Нефедов В.И. Общая теория связи. – М.: Издательство Юрайт. 2020.-495 с.
5. Нефедов В.И. Теория электросвязи.- М.: Издательство Юрайт. 2020.-495 с.
6. Мельников Д.А. Системы и сети передачи данных. – М.: ИП РадиоСофт, 2019.-624.
7. Ситников А.В. Электротехнические основы источников питания. – М.: «Академия», 2019. – 240 с.
8. Хрусталева З.А. Электрические и электронные измерения в задачах, вопросах и упражнениях. – М.: «Академия», 2019. – 176 с.

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

Сайт Научной электронной библиотеки www.elibrary.ru

http:/www.globus-telecom.com

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники:

Отечественные журналы:

- «Электросвязь»;
- «Вестник связи»;
- «Сети и системы связи»;
- «Инфокоммуникационные технологии»;
- «Технологии и средства связи».

Справочные пособия:

- ГОСТ 8.417-2002. ГСИ. «Единицы величин».
- ГОСТ Р 1.0-2004. «Стандартизация в РФ. Основные положения»
- ГОСТ Р 8.563-96. ГСИ «Методики выполнения измерений»
- Закон РФ «О техническом регулировании».
- Правила по проведению сертификации в РФ.
- Порядок проведения сертификации продукции в РФ.
- ГОСТ 8.417-2002 Государственная система обеспечения единства измерений. Единицы величин.
- ГОСТ Р 8.000-2001 Государственная система обеспечения единства измерений. Основные положения.
- ОСТ 45.159-2000 Отраслевая система обеспечения единства измерений. Термины и определения.
- ОСТ 45.150-99 Методики выполнения измерений. Порядок разработки и аттестации.
- ГОСТ Р 40.001-93 Система сертификации ГОСТ Р. Регистр систем качества. Основные положения.
- ГОСТ Р 1.0-92 Государственная система стандартизации РФ. Основные положения.
- www.Convertworld.com (перевод единиц измерения)

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы 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;	Экспертное наблюдение
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, поиску неисправностей и ремонту	Экспертное наблюдение
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; - производить контроль и регулировку основных параметров источников питания оборудования ИТКС;	Экспертное наблюдение
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.	Экспертное наблюдение

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Экспертное наблюдение Экзамен
ОК 2.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством,	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

\

Приложение 1.2
к программе СПО
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности организовывать ремонтные, монтажные и наладочные работы по промышленному оборудованиюи соответствующие ему профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1	**Защита информации в информационно-телекоммуникационных системах и сетях 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.	Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе криптографических средств защиты информации в информационно-телекоммуникационных системах и сетях.
ПК 2.3.	Осуществлять защиту информации от несанкционированного доступа и специальных воздействий в оборудование информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

1.1.1. Общие компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
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 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном языке.

В результате освоения профессионального модуля студент должен:

Иметь Навыки	– определения необходимых средств криптографической защиты информации; – использования программно-аппаратных криптографических средств защиты информации; – установки, настройки специализированного оборудования криптографической защиты информации; – применения программно-аппаратных средств обеспечения информационной безопасности телекоммуникационных систем; – шифрования информации.
уметь	– выявлять и оценивать угрозы безопасности информации и возможные технические каналы ее утечки на конкретных объектах; – определять рациональные методы и средства защиты на объектах и оценивать их эффективность; – производить установку и настройку типовых программно-аппаратных средств защиты информации; – пользоваться терминологией современной криптографии, использовать типовые криптографические средства защиты информации;
знать	– типовые криптографические алгоритмы, применяемые в защищенных телекоммуникационных системах; – основные протоколы идентификации и аутентификации в телекоммуникационных системах; – состав и возможности типовых конфигураций программно-аппаратных средств защиты информации; – особенности применения программно-аппаратных средств обеспечения информационной безопасности в телекоммуникационных системах; – основные способы противодействия – несанкционированному доступу к информационным ресурсам информационно-телекоммуникационной системы; – основные понятия криптографии и типовые криптографические методы защиты информации;

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: 673 часов.

Из них на освоение МДК – 613 часов:

МДК.02.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты- 290 часов;

в том числе самостоятельная работа 122 часа;

МДК.02.02 Криптографическая защита информации - 176 часов;

в том числе самостоятельная работа 44 часа;

На практики, в том числе учебная 36 часов

производственная -108 часа.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе					
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация	Учебная	Производственная
1	*2*	*3*	*4*	*5*	*6*		*7*	*8*	*9*	*10*
ПК 2.1-2.3 ОК 1 – 5, ОК 9,10	Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты	**290**		**290**	106		122			
ПК 2.1-2.3 ОК 1 – 5, ОК 9,10	Раздел 2. Криптографическая защита информации	**176**		**176**	67		44			

ПК 2.1-2.3 ОК 1 – 5, ОК 9,10	Учебная практика	**36**							**36**	
ПК 2.1-2.3 ОК 1 – 5, ОК 9,10	Производственная практика	**108**								**108**
	Промежуточная аттестация	**18**								
	Всего:	***628***		***466***	***173***		***166***		***36***	***108***

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект)	Объем часов	Код ПК, ОК
1	**2**	**3**	
ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты		**628**	
Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		**290**	
МДК 02.01. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты		290	
Тема 1.1. Обеспечение безопасности операционных систем	**Содержание**		ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows XP. Windows 7. Windows8. Linux. QNX и другие операционные системы. Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователя. Методы аутентификации. Пароли. PIN-коды. Методы надежного составления паролей. Строгая аутентификация. Односторонняя аутентификация. Двухсторонняя аутентификация Аппаратно-программные средства идентификации и аутентификации. Токены. Смарт-карты. Виртуальные ключи. Программно-аппаратные модули доверенной загрузки. Задачи АПМДЗ. Возможности АПМДЗ. Виды АПМДЗ. АПМДЗ Криптон –Замок системный администратор. Изучение настроек системного администратора АПМДЗ. АПМДЗ Криптон –Замок, настройки пользователя АПМДЗ. Ограничения действий пользователя. Идентификация. Журнал регистрации событий. Настройки целостности среды АПМДЗ Сектор НЖМД. Область памяти. Файл, папка, каталог.	10	
	Практические занятия	**26**	

	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows.Политика паролей. Политики учетных записей. Назначение прав пользователя Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита Настройка изолированной среды АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование Восстановление информации типовыми средствами Программы восстановление информации	26	
Тема 1.2. Технологии разграничения доступа	**Содержание**	**10**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Архитектура подсистемы защиты операционной системы Windows Server2016. Особенности ОС Windows Server2016. Возможности администратора. Разграничение доступа к объектам операционной системы. Модели доступа. Дискреционная модель. Мандатная модель. Роли. Локальная политика безопасности. Настройка локальной политики безопасности. Администрирование системы. Изолированная программная среда. Способы организации. Методы применения. ActiveDirectory. Комплексная система организации управления доступом. Инсталяция. Настройка. Аудит безопасности операционной системы. Методы проведения контрольных проверочных мероприятий. Программные средства аудита. Функции межсетевых экранов. Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. Особенности функционирования межсетевых экранов. Модель OSI. Экранирующий маршрутизатор. Шлюз сеансового уровня. Прикладной шлюз. Шлюз экспертного уровня. Схемы защиты на базе межсетевых экранов. Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. Проблемы безопасности МЭ. Тестирование межсетевых экранов. Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ.		

	Практические занятия	**20**	
	Программы надежного удаления информации Архивирование информации Программные средства резервного копирования. Настройка RAID-массивов Инсайдерская информация. Программы сбора информации о ПК Настройка межсетевого экрана	20	
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	**Содержание**	**16**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Проблемы информационной безопасности сетей. Введение в сетевой информационный обмен. Использование сети Интернет. Модель ISO/OSI и стек протоколов TCP/IP. Обеспечение информационной безопасности сетей. Способы обеспечения информационной безопасности. Пути решения проблем защиты информации в сетях. Концепция построения виртуальных защищенных сетей. Надежная передача информации по незащищенным каналам связи. Шифрование. Аутентификация. Верификация. Избыточное кодирование. VPN – решения для построения защищенных сетей. Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура пакета. Структура защищенного пакета. Варианты построения защищенных каналов. Классификация. Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. Протоколы формирования защищенных каналов на сеансовом уровне. протоколы SSL, TLS, SOCKS. Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. Защита на прикладном уровне. Организация удаленного доступа. Управление идентификацией и доступом. Средства управления доступом. Web-доступ. Протоколы PAP, CHAP, S/Key, SSO, Kerberos.		
	Практические занятия	46	
	Основные действия с виртуальной машиной Работа с контрольными точками Использование внешних устройств Работа с локальным хранилищем сертификатов в ОС WINDOWS Установка и настройка ПО eTokenPKIClient Настройка ПО eTokenPKIClient с помощью групповых политик Развертывание TMS в среде Active Directory Настройка TMS в среде Active Directory Настройка политик TMS Настройка использования виртуального токена Использование токена на рабочем месте	46	

	администратора Установка и настройка СКЗИ «КриптоПроCSP» Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP Применение SecretDisk4 Применение SecretDisk Server NG Изучение основных возможностей ПО VipNetClient Изучение настроек ПО VipNetClient Изучение возможностей ПО Деловая почта		
Тема 1.4. Технологии обнаружения вторжений	**Содержание**	**14**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Технология обнаружения атак. Концепция адаптивного управления безопасностью. Технология анализа защищенности. Средства анализа защищенности сетевых протоколов и сервисов. Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности. Средства обнаружения сетевых атак. Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки. Обзор современных средств обнаружения атак. Технологии защиты от вирусов. Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов. Основные каналы распространения вирусов и других вредоносных программ.		
	Практические занятия	**14**	
	Изучение средств обнаружения атак Изучение антивирусных продуктов	14	
Тема 1.5. Методы управления средствами защиты	**Содержание**	**12**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Методы управления средствами сетевой защиты. Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты. Аудит безопасности информационной системы. Мониторинг безопасности системы. Программные средства проведения аудита безопасности. Обзор современных систем управления сетевой защитой. Классификация систем защиты. Перспективы и тенденции в развитии систем защиты.		
Самостоятельная учебная работа		122	ПК 2.1-2.3 ОК 1 – 5, ОК
Тематика самостоятельной работы:			

1. Проблемы обеспечения безопасности операционных систем Windows XP. Windows 7. Windows8. Linux. QNX. 2.Технологии аутентификации. 3.Аутентификация, авторизация и администрирование действий пользователя. 4.Пароли. PIN-коды. Методы надежного составления паролей. 5.Токены. Смарт-карты. Виртуальные ключи. 6.Программно-аппаратные модули доверенной загрузки. 7.АПМДЗ Криптон –Замок системный администратор. 8.Изучение настроек системного администратора АПМДЗ. 9.Сектор НЖМД. Область памяти. Файл, папка, каталог. 10.Разграничение доступа к объектам операционной системы. 11.Комплексная система организации управления доступом. Инсталяция. Настройка. 12.Аудит безопасности операционной системы. 13.Функции межсетевых экранов.Ограничение доступа внешних пользователей. Разграничение доступа. Фильтрация трафика. 14.Анализ информации. Пакетная фильтрация. Посреднические функции. Дополнительные возможности МЭ. 15.Политика межсетевого взаимодействия. Схемы подключения МЭ. Персональные и распределенные МЭ. 16.Требования показателей тестирования. Классы МЭ. Требования ФСТЭК к МЭ. 17.Концепция построения виртуальных защищенных сетей. 18.Виртуальные защищенные сети. Тунелирование. Инкапсуляция пакетов. Структура защищенного пакета. Варианты построения защищенных каналов. 19.Защита на канальном уровне. Протоколы PPTP, L2F, L2TP. 20.Протоколы формирования защищенных каналов на сеансовом уровне. Протоколы SSL, TLS, SOCKS. 21.Защита на сетевом уровне. Архитектура средств безопасности IPSec, AH, ESP. 22.Защита на прикладном уровне. ПротоколыPAP, CHAP,S/Key, SSO, Kerberos. 23.Функционирование системы управления средствами защиты. 24.Аудит безопасности информационной системы.		9,10
Учебная практика раздела МДК02.01. **Виды работ:**	36	ПК 2.1-2.3 ОК 1 – 5, ОК

Выбор, подключение, настройка межсетевого экрана. Администрирование межсетевого экрана. Ознакомление, подключение, настройка системы резервного копирования Администрирование системы резервного копирования. Ознакомление, подключение, настройка системы антивирусной защиты. Администрирование системы антивирусной защиты.			9,10
Раздел 2. Криптографическая защита информации		**144**	
МДК 02.02. Криптографическая защита информации		144	
Тема 2.1. Основы криптографических методов защиты информации	**Содержание**		ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Свойства информационной безопасности. Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности. Криптографические методы. Шифрование. Кодирование. Стеганография. Сжатие. Математика криптографии. Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение. Традиционные шифры перестановки. Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования. Традиционные шифры замены. Шифры замены. Шифры многоалфавитной замены. Частотность символов. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. Компьютерное шифрование. Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей.	**16**	
	Практические занятия	**27**	
	Стеганографические методы скрытия информации Бинарная арифметика. Модульная арифметика Применение методов шифрования перестановкой Применение методов шифрования заменой Применение методов шифрования многоалфавитной замены Криптоанализ методов перестановки Криптоанализ методов замены Компьютерное шифрование	27	
Тема 2.2. Современные	**Содержание**	**17**	ПК 2.1-2.3

стандарты шифрования	Симметричное шифрование. Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES. Усовершенствованный стандарт шифрования AES. Структура AES. Расширение ключей 128/192/256. Анализ безопасности AES. Российские стандарты симметричного шифрования. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. Проблема распределения ключей симметричного шифрования. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. Асимметричное шифрование. Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. Российские стандарты асимметричного шифрования. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов.		ОК 1 – 5, ОК 9,10
	Практические занятия	**16**	
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	16	
Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	**Содержание**	**18**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
	Целостность сообщения. Случайная модель Orac1e. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SHA-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции. Электронная цифровая подпись. Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП.ГОСТ Р 34.10 -2012. Установление подлинности объекта. Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены. Проблемы распределения открытого ключа асимметричного шифрования. Сертификаты открытого ключа.		

	Удостоверяющие центры. X.509. Иерархия PKI. Обеспечение безопасности сети с применением криптографических протоколов на прикладном уровне. Электронная почта. Архитектура e-mail. PGP. S/M1ME. Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне. Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети Защита информации в сетях, организованных по технологии беспроводного доступа. IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16. Защита информации в сетях сотовой связи. A3. A8.A5/3. Атаки на алгоритмы. Перспективы развития беспроводной мобильной связи. Криптовалюты. Биткоин. Блокчейн-системы Ethereum. Перспективы развития криптографии. Квантовая криптография. Проблемы ограничения скорости шифрования. Проблемы теории асимметричных алгоритмов.		
	Практические занятия	**24**	
	Разработка хэш-функции Разработка схемы простого пароля Разработка схемы динамического пароля Сертификаты открытого ключа Настройка и администрирование токена Настройка сервисов Рутокен-PinPad Настройка сервисов Рутокен-ЭЦП Настройка сервисов Рутокен–Bluetooth Настройка сервисов Рутокен–S Разработка алгоритма PGP Изучение протоколов SSL, TLS, IPSec Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	24	
Самостоятельная учебная работа при изучении раздела ПМ		**44**	
Тематика самостоятельной работы: 1. Изучение новых технологий хранения информации. 2. Статистика и анализ крупных утечек информации за год. 3. Поиск информации о новых видах атак на информационную систему. 4. Обзор современных программных и программно-аппаратных средств защиты. 5. Сравнительный анализ современных программных и программно-аппаратных средств защиты. 6. Криптографические методы. 7. Шифрование. Кодирование. Стеганография. Сжатие. 8. Традиционные шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. 9.Традиционные шифры замены. Шифры многоалфавитной замены. Частотность символов.		44	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10

10. Криптоанализ. Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста. 11. Компьютерное шифрование. 12. Стандарт шифрования данных DES. Структура DES. Безопасность DES. Структура ГОСТ 28147-89. Режимы шифрования ГОСТ 28147-89. Анализ безопасности ГОСТ 28147-89. ГОСТ Р 34.12-2015. 13. Алгоритм Диффи-Хелмана. Управление ключами. Kerberos. 14. Асимметричное шифрование. Криптографическая система Эль-Гамаля. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012.		
Производственная практика **Виды работ** Участие в организации работ по защите персональных компьютеров на предприятии Участие в организации работ по защите локальных сетей на предприятии Участие в организации работ по защите работ в глобальной сети интернет на предприятии Ознакомление, организация, настройка систем безопасности проводной защищенной локальной сети. Администрирование систем безопасности проводной защищенной локальной сети. Ознакомление, организация, настройка систем безопасности беспроводной защищенной локальной сети. Администрирование систем безопасности беспроводной защищенной локальной сети. Поддержание бесперебойной работы программных и программно-аппаратных, в том числе криптографических средств защиты информации в оборудовании информационно-телекоммуникационных систем и сетей. Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Выбор программных средств шифрования в соответствии с решаемой задачей Подключение, установка драйверов, настройка программных средств абонентского шифрования Администрирование внедренных средств Настройка средств электронной подписи Администрирование средств электронной подписи Администрирование средств PKI	**108**	ПК 2.1-2.3 ОК 1 – 5, ОК 9,10
Промежуточная аттестация	**18**	
Всего по ПМ	**628**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

Реализация программы профессионального модуля требует наличия учебных кабинетов, лабораторий:

Лаборатория «Программных и программно-аппаратных средств защиты информации».

Лаборатория должна быть оснащена антивирусными программными комплексами; аппаратными средствами аутентификации пользователя; программно-аппаратными средствами управления доступом к данным и защиты (шифрования) информации; средствами защиты информации от НСД, блокирования доступа и нарушения целостности; программными средствами криптографической защиты информации; программными средствами выявления уязвимостей и оценки защищенности ИТКС, анализа сетевого трафика;

системы разграничения доступа;

межсетевые экраны;

средство криптографической защиты информации, реализующее функции удостоверяющего центра и создания виртуальных сетей;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябовд.Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2019. – 363 с.

2.Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов, 5-е изд. – Спб.: Питер, 2019 – 944 с.

3.Томаси У. Электронные системы связи.- М.: Техносфера, 2019. -1360с.

4.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2019. – 184 с.

5.Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2019. – 172 с.

6.Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/ Е.Б. Белов, В.Н. Пржегорлинский. – М.: Издательский центр «Академия», 2019. – 336с

7.В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2019

8.Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

9.Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2019. - 192с.

10.Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2019. – 416 с.

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

Дополнительные источники:

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

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

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

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

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

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

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

–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».

– Положение о сертификации средств защиты информации. Утверждено

постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

– 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.

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

– 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.

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

– 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.

– 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.

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

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

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

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

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

– 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.

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

– 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

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

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

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

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

– 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

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

– 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

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

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

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

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

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

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

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

– 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.

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

– 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.

– 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 ISO/IEC 15408-2:2008). Росстандарт, 2013.

– Методика определения актуальных угроз безопасности персональных данных при

их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

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

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

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

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

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

Отечественные журналы:

"InformationSecurity/ Информационная безопасность"

Системный администратор

Компьютер ПРЕСС

Системы безопасности. Журнал для руководителей и специалистов в области безопасности

Сети и системы связи

Защита информации. Инсайд: Информационно-методический журнал

Информационная безопасность регионов: Научно-практический журнал

Интернет Ресурсы

http://cryptogrof.ru/

4. Контроль и оценка результатов освоения профессионального модуля

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Осуществлять установку (монтаж), настройку (наладку) и запуск в эксплуатацию программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности 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 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	Экспертное наблюдение
ПК 2.2. Обеспечивать эксплуатацию и содержание в работоспособном состоянии программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности ИТКС и их диагностику, обнаружение отказов, формировать предложения по их устранению	- 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 программно-аппаратных (в том числе криптографических) средств защиты информации;	Экспертное наблюдение

ПК 2.3. Формулировать предложения по применению программно-аппаратных и инженерно-технических средств обеспечения информационной безопасности 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;	Экспертное наблюдение
ПК 2.4. Вести рабочую техническую документацию по эксплуатации средств и систем обеспечения информационной безопасности телекоммуникационных систем, осуществлять своевременное списание и пополнение	- 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;	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством,	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен
ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

Приложение 1.3

к программе СПО

10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить вид деятельности и соответствующие ему общие и профессиональные компетенции:

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических 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.

1.1.1. Общие компетенции

Код	Наименование видов деятельности и профессиональных компетенций
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 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь Навыки	установка, монтаж и настройка технических средств защиты информации; техническое обслуживание технических средств защиты информации; применение основных типов технических средств защиты информации; выявление технических каналов утечки информации; участие в мониторинге эффективности технических средств защиты информации; диагностика, устранение отказов и неисправностей, восстановление работоспособности технических средств защиты информации; проведение измерений параметров ПЭМИН, создаваемых техническими средствами обработки информации при аттестации объектов информатизации; проведение измерений параметров фоновых шумов, а также физических полей, создаваемых техническими средствами защиты информации; установка, монтаж и настройка, техническое обслуживание, диагностика, устранение отказов и неисправностей, восстановление работоспособности инженерно-технических средств физической защиты.
Уметь	применять технические средства для криптографической защиты информации конфиденциального характера; применять технические средства для уничтожения информации и носителей информации; применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных; применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; применять инженерно-технические средства физической защиты объектов информатизации
Знать	порядок технического обслуживания технических средств защиты информации; номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; физические основы формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; структуру и условия формирования технических каналов утечки информации; порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; основные принципы действия и характеристики технических средств физической защиты; основные способы физической защиты информации; номенклатуру применяемых средств физической защиты объектов информатизации.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов: 560 часов.

Из них на освоение МДК –511 часов:

МДК.03.01 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты – 190 часов;

в том числе самостоятельная работа 47 часов;

МДК.03.02 Физическая защита линий связи информационно-телекоммуникационных систем и сетей - 123 часа;

в том числе самостоятельная работа 19 часов;

На практики, в том числе учебная 72 часа

производственная -108 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуляПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Коды профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего, час.	В т.ч. в форме практической подготовки	Объем профессионального модуля, ак. час.						
				Обучение по МДК					Практики	
				Всего	В том числе					
					Лабораторных и практических занятий	Курсовых работ (проектов)	Самостоятельная работа	Промежуточная аттестация	Учебная	Производственная
1	*2*	*3*	*4*	*5*	*6*		*7*	*8*	*9*	*10*
ПК 3.1-3.4 ОК 1 – 5, ОК 9,10	Раздел 1. Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты	**190**		**190**	94		47			
ПК 3.1-3.4 ОК 1 – 5, ОК 9,10	Раздел 2. Физическая защита линий связи информационно-телекоммуникацио	**123**		**123**	52		19			

	нных систем и сетей									
ПК 3.1-3.4 ОК 1 – 5, ОК 9,10	Учебная практика	**72**							**72**	
ПК 3.1-3.4 ОК 1 – 5, ОК 9,10	Производственная практика	**108**								**108**
	Промежуточная аттестация	**36**								
	Всего:	***529***		***313***	***146***		***66***		***36***	***108***

2.2. Тематический план и содержание профессионального модуля ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объем часов	
1	2	3	
Раздел 1. Защита информации в ИТКС с использованием технических средств защиты		**190**	
МДК.03.01. Защита информации в ИТКС с использованием технических средств защиты		190	
Тема 1.1. Предмет и задачи технической защиты информации	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Предмет и задачи технической защиты информации. Характеристика инженерно-технической защиты информации как области информационной безопасности. Системный подход при решении задач инженерно-технической защиты информации. Основные параметры системы защиты информации.		
Тема 1.2. Общие положения защиты информации техническими средствами	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Задачи и требования к способам и средствам защиты информации техническими средствами. Принципы системного анализа проблем инженерно-технической защиты информации. Классификация способов и средств защиты информации.		
Тема 2.1. Информация как предмет защиты	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации. Демаскирующие признаки объектов наблюдения, сигналов и веществ. Понятие об опасном сигнале. Источники опасных сигналов. Основные и вспомогательные технические средства, и системы. Основные руководящие, нормативные и методические документы по защите информации и противодействию технической		

	разведке.		
	Практические занятия	**2**	
	Содержательный анализ основных руководящих, нормативных и методических документов по защите информации и противодействию технической разведке.	2	
Тема 2.2. Технические каналы утечки информации	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.		
	Практические занятия	**4**	
	Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации	4	
Тема 2.3. Методы и средства технической разведки	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.		
	Практические занятия	**4**	
	Тематика учебных занятий формируется образовательной организацией самостоятельно		
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	**Содержание**	**6**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Физические основы побочных электромагнитных излучений и наводок. Акустоэлектрические преобразования. Паразитная генерация радиоэлектронных средств. Виды паразитных связей и наводок. Физические явления, вызывающие утечку информации по цепям электропитания и заземления. Номенклатура и характеристика аппаратуры, используемой для измерения параметров побочных электромагнитных излучений и наводок, параметров фоновых шумов и физических полей		
	Практические занятия	**6**	
	Измерение параметров физических полей	6	
Тема 3.2. Физические	**Содержание**	**2**	ПК 3.1-3.4

процессы при подавлении опасных сигналов	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.		ОК 1 – 5, ОК 9,10
	Практические занятия	**4**	
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований.	4	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	**Содержание**	**3**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Технические средства акустической разведки. Непосредственное подслушивание звуковой информации. Прослушивание информации направленными микрофонами. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.		
	Практические занятия	**10**	
	Защита от утечки по акустическому каналу	10	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Принцип работы микрофона и телефона. Использование коммуникаций в качестве соединительных проводов. Негласная запись информации на диктофоны. Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу.		
	Практические занятия	**4**	
	Использование коммуникаций в качестве соединительных проводов	4	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Электронные стетоскопы. Лазерные системы подслушивания. Гидроакустические преобразователи. Системы защиты информации от утечки по вибрационному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по вибрационному каналу.		
	Практические занятия	**10**	
	Защита от утечки по виброакустическому каналу	10	
Тема 4.4. Системы защиты от утечки информации по	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники		

электромагнитному каналу	информации с радиозакладок. Прослушивание информации о пассивных закладок. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.		
	Практические занятия	**8**	
	Определение каналов утечки ПЭМИН	8	
	Защита от утечки по цепям электропитания и заземления		
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу.		
	Практические занятия	**4**	
	Использование микрофона телефонного аппарата при положенной телефонной трубке.	4	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.		
	Практические занятия	**10**	
	Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу	10	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.		
	Практические занятия	**2**	
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	**4**	
Тема 5.1. Применение технических средств	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК
	Технические средства для уничтожения информации и носителей информации, порядок		

защиты информации	применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации.		9,10
	Практические занятия	**10**	
	Проведение измерений параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации	10	
Тема 5.2. Эксплуатация технических средств защиты информации	**Содержание**	**4**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Этапы эксплуатации технических средств защиты информации. Виды, содержание и порядок проведения технического обслуживания средств защиты информации. 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.		
	Практические занятия	**16**	
	Диагностика, устранение отказов и восстановление работоспособности технических средств защиты информации. Организация ремонта технических средств защиты информации	16	
Самостоятельная учебная работа при изучении раздела 1 ПМ		**47**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
Тематика самостоятельной работы: 1. Классификация способов и средств защиты информации. 2. Основные и вспомогательные технические средства, и системы. 3. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. 4. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика. 5. Система защиты от утечки по акустическому каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по акустическому каналу.			

6. . Системы защиты от диктофонов. Номенклатура применяемых средств защиты информации от несанкционированной утечки по проводному каналу. 7. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу. 8. Технические средства для уничтожения информации и носителей информации, порядок применения.			
Раздел 2. Физическая защита линий связи ИТКС		**123**	
МДК.03.02. Физическая защита линий связи ИТКС		**123**	
Тема 1.1. Цели и задачи физической защиты объектов информатизации	**Содержание**	**5**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Характеристики потенциально опасных объектов. Содержание и задачи физической защиты объектов информатизации. Основные понятия инженерно-технических средств физической защиты. Категорирование объектов информатизации. Модель нарушителя и возможные пути, и способы его проникновения на охраняемый объект. Особенности задач охраны различных типов объектов.		
	Практические занятия	**4**	
	Категорирование объектов информатизации	4	
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	**Содержание**	**5**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Общие принципы обеспечения безопасности объектов. Жизненный цикл системы физической защиты. Принципы построения интегрированных систем охраны. Классификация и состав интегрированных систем охраны. Требования к инженерным средствам физической защиты. Инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации.		
	Практические занятия	**6**	
	Классификация и состав интегрированных систем охраны	12	
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	**Содержание**	**6**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия.		

	Практические занятия	**8**	
	Монтаж датчиков пожарной и охранной сигнализации	8	
Тема 2.2. Система контроля и управления доступом	**Содержание**	**2**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Место системы контроля и управления доступом (СКУД) в системе обеспечения информационной безопасности. Особенности построения и размещения СКУД. Структура и состав СКУД. Периферийное оборудование и носители информации в СКУД. Основы построения и принципы функционирования СКУД. Классификация средств управления доступом. Средства идентификации и аутентификации. Методы удостоверения личности, применяемые в СКУД. Обнаружение металлических предметов и радиоактивных веществ.		
	Практические занятия	**6**	
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	3	
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	3	
Тема 2.3. Система телевизионного наблюдения	**Содержание**	**6**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.		
	Практические занятия	**6**	
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6	
Тема 2.4. Система сбора, обработки, отображения и документирования информации	**Содержание**	**6**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства отображения и документирования информации.		
	Практические занятия	**2**	
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2	
Тема 2.5. Система воздействия	**Содержание**	**6**	ПК 3.1-3.4 ОК 1 – 5, ОК
	Назначение и классификация технических средств воздействия. Основные показатели		

	технических средств воздействия.		9,10
	Практические занятия	**6**	
	Классификация технических средств воздействия	6	
Тема 3.1. Применение инженерно-технических средств физической защиты	**Содержание**		ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Периметровые и объектовые средства обнаружения, порядок применения. Работа с периферийным оборудованием системы контроля и управления доступом. Особенности организации пропускного режима на КПП. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	**6**	
	Практические занятия	**7**	
	. Управление системой телевизионного наблюдения с автоматизированного рабочего места. Порядок применения устройств отображения и документирования информации. Управление системой воздействия.	7	
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	**Содержание**		ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
	Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	**6**	
	Практические занятия		
	Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.	**6**	
Самостоятельная учебная работа при изучении раздела модуля 2 Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем) Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчетов к их защите.		**19**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
Учебная практика по профессиональному модулю		***72***	ПК 3.1-3.4

1. Монтаж различных типов датчиков. 2. Проектирование установки системы пожарно-охранной сигнализации по заданию и ее реализация. 3. Применение промышленных осциллографов, частотомеров и генераторов и другого оборудования для защиты информации. 4. Рассмотрение системы контроля и управления доступом. 5. Рассмотрение принципов работы системы видеонаблюдения и ее проектирование. 6. Рассмотрение датчиков периметра, их принципов работы. 7. Выполнение звукоизоляции помещений системы зашумления. 8. Реализация защиты от утечки по цепям электропитания и заземления. 9. Разработка организационных и технических мероприятий по заданию преподавателя; 10. Разработка основной документации по инженерно-технической защите информации.		ОК 1 – 5, ОК 9,10
Производственная практика профессионального модуля **Виды работ** 1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации; 2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения; 3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам; 4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами.	**108**	ПК 3.1-3.4 ОК 1 – 5, ОК 9,10
Промежуточная аттестация	**36**	
Всего по ПМ	**529**	

3.УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрены следующие специальные помещения

Лаборатория«Защиты информации от утечки по техническим каналам».

Лаборатория должна быть оснащена средствами защиты информации от утечки по акустическому (виброакустическому) каналу; средствами защиты информации от утечки по каналам, формируемым за счет побочных электромагнитных излучений и наводок; средствами контроля эффективности защиты информации от утечки по акустическому (виброакустическому) каналу и каналам побочных электромагнитных излучений и наводок;

шумогенераторы;

комплексный поисковый прибор;

прожигатели телефонных линий;

устройство обнаружения скрытых видеокамер;

виброакустические генераторы;

подавители диктофонов;

подавители устройств сотовой связи;

устройство защиты аналоговых сигналов;

устройство защиты цифровых сигналов;

стенды физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения, охранно-пожарной сигнализации и охраны объектов;

комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном).

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

3.2.1. Печатные издания

1. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. 7-е изд., испр. 20149
2. Пеньков Т.С. Основы построения технических систем охраны периметров. Учебное пособие. — М. 2019
3. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 1. Правовое обеспечение информационной безопасности: учеб. Пособие. – М.: МИЭТ, 2019. – 184 с.
4. Новиков В.К. Организационное и правовое обеспечение информационной безопасности: В 2-х частях. Часть 2. Организационное обеспечение информационной безопасности: учеб.пособие. – М.: МИЭТ, 2019. – 172 с.
5. Е.Б. Белов, В.Н. Пржегорлинский Организационно-правовое обеспечение информационной безопасности: учеб.пособие для студ. учреждений сред. проф. образования/. – М.: Издательский центр «Академия», 2019. – 336с
6. Ю.Ю. Коваленко. Правовой режим лицензирования и сертификации в сфере информационной безопасности: Учебное пособие / – М.: Горячая линия – Телеком, 2019.

7. Электронный конспект лекций «Инженерно-техническая защита информации». Составитель: И.Н. Драч, преподаватель ГБОУ СПО РО «РКСИ»

8. Электронный конспект лекций «Криптографическая защита информации». Составитель: Шигаева С.В., преподаватель ГБОУ СПО РО «РКСИ»

9. Иванов М.А., Чугунков И.В. Криптографические методы защиты информации в компьютерных системах и сетях. Учебное пособие - Москва: МИФИ, 2019.- 400 с. Рекомендовано УМО «Ядерные физика и технологии» в качестве учебного пособия для студентов высших учебных заведений.

10. В.П. Мельников, С.А. Клейменов, А.М. Петраков: Информационная безопасность и защита информации М.: Академия, - 336 с. – 2019

11. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях Изд-во: ДМК Пресс, - 2019

12. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности: учебник: Рекомендовано УМО, 2019. - 192с.

13. Каторин Ю.Ф., Разумовский А.В., Спивак А.И. Защита информации техническими средствами: Учебное пособие / Под редакцией Ю.Ф. Каторина – СПб: НИУ ИТМО, 2019. – 416 с.

3.2.2. Электронные издания (электронные ресурсы)

Интернет-ресурсы:

Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

http://www.morion.ru/

http://www.nateks.ru/

http://www.iskratel.com/

http://www.ps-ufa.ru/

http://3m.com/

http://www.rusgates.ru/index/php - Материалы сайта завода «Ферроприбор»

3.2.3. Дополнительные источники

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

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

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

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

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

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

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

– 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».

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

– 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.

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

– 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.

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

– 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.

– 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.

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

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

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

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

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

– 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.

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

– 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

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

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

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

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

– 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

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

– 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

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

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

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

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

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

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

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

– 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.

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

– 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.

– 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 ISO/IEC 15408-2:2008). Росстандарт, 2013.

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

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

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

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

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

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

Отечественные журналы:

"InformationSecurity/ Информационная безопасность"
Системный администратор
Компьютер ПРЕСС
Системы безопасности. Журнал для руководителей и специалистов в области безопасности
Сети и системы связи

Интернет Ресурсы

http://cryptogrof.ru/

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Производить установку, монтаж, настройку и испытания технических средств защиты информации от утечки по техническим каналам в ИТКС.	- 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;	Экспертное наблюдение
ПК 3.2. Проводить техническое обслуживание, диагностику, устранение неисправностей и ремонт технических средств защиты информации, используемых в	- 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	Экспертное наблюдение
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;	Экспертное наблюдение

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	Экспертное наблюдение
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач;	Экспертное наблюдение Экзамен
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения; - обоснованность самоанализа и коррекция результатов собственной работы;	Экспертное наблюдение Экзамен
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами,	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных);	Экспертное наблюдение Экзамен
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Экспертное наблюдение Экзамен

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Экспертное наблюдение Экзамен

Приложение 1.4
к программе СПО
10.02.04 Обеспечение информационной безопасности телекоммуникационных систем

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих»

2025 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

«ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих 16199 Оператор электронно-вычислительных и вычислительных машин»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
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 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 4	Выполнять работы по профессии «Оператор электронно-вычислительных и вычислительных машин»

ПК 4.1.	Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения
ПК 4.2.	Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах
ПК 4.3.	Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета
ПК 4.4.	Обеспечивать применение средств защиты информации в компьютерной системе

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	выполнения требований техники безопасности при работе с вычислительной техникой; организации рабочего места оператора электронно-вычислительных и вычислительных машин; подготовки оборудования компьютерной системы к работе; инсталяции, настройки и обслуживания программного обеспечения компьютерной системы; управления файлами; применения офисного программного обеспечения в соответствии с прикладной задачей; использования ресурсов локальной вычислительной сети; использования ресурсов, технологий и сервисов Интернет; применения средств защиты информации в компьютерной системе.
уметь	выполнять требования техники безопасности при работе с вычислительной техникой; производить подключение блоков персонального компьютера и периферийных устройств; производить установку и замену расходных материалов для периферийных устройств и компьютерной оргтехники; 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; использовать мультимедиа проектор для демонстрации презентаций; вводить, редактировать и удалять записи в базе данных; эффективно пользоваться запросами базы данных; создавать и редактировать графические объекты с помощью программ для обработки растровой и векторной графики; производить сканирование документов и их распознавание; производить распечатку, копирование и тиражирование документов на принтере и других устройствах; управлять файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети и в интернете; осуществлять навигацию по Веб-ресурсам Интернета с помощью браузера; осуществлять поиск, сортировку и анализ информации с помощью поисковых интернет сайтов; осуществлять антивирусную защиту персонального компьютера с помощью антивирусных программ. осуществлять резервное копирование и восстановление данных
знать	требования техники безопасности при работе с вычислительной техникой; основные принципы устройства и работы компьютерных систем и периферийных устройств; классификацию и назначение компьютерных сетей; виды носителей информации; программное обеспечение для работы в компьютерных сетях и с ресурсами Интернета; основные средства защиты от вредоносного программного обеспечения и несанкционированного доступа к защищаемым ресурсам компьютерной системы.

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов 315

Из них на освоение МДК 284 часов

В том числе,

на практики, в том числе учебную 144часа

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональных общих компетенций	**Наименования разделов профессионального модуля**	**Суммарный объем нагрузки, час.**	**Объем профессионального модуля, ак. час.**					
			Работа обучающихся во взаимодействии с преподавателем					**Самостоятельная работа**
			Обучение по МДК			**Практики**		
			Всего	**В том числе**		**Учебная**	**Производственная**	
				Лабораторных и практических занятий	**Курсовых работ (проектов)1**			
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
ПК 4.1 – ПК 4.4 ОК1–ОК 10	Раздел 1 модуля. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»	315	254	101	-	72	72	4
	Всего:	315	284	101	-	72	72	4

Промежуточная аттестация: экзамен (квалификационный)

2.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	**Содержание учебного материала,** **лабораторные работы и практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся**	**Объем часов**
1	2	3
Раздел модуля 1. Выполнение работ по рабочей профессии «Оператор электронно-вычислительных и вычислительных машин»		315
МДК.04.01. Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих 16199 Оператор электронно-вычислительных и вычислительных машин		284
Раздел 1. Подготовка оборудования компьютерной системы к работе, инсталляция, настройка и обслуживание программного обеспечения		23
Тема 1.1. Работа с устройствами компьютерной системы	Содержание	4
	Соблюдение техники безопасности при работе на ЭВМ Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка Установка и замена расходных материалов для принтеров, ксерокса, плоттера.	1 1 1 1
	Тематика практических занятий	5
	Изучение архитектуры ЭВМ, структуры и основных принципов работы ЭВМ Работа с дополнительными внешними устройствами ПК: поиск драйверов, подключение, настройка	3 2
	Практическая подготовка	4
Тема 1.2.	Содержание	4

Работа с программным обеспечением компьютерной системы	Установка операционной среды, настройка интерфейса операционной системы (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети, в Интернете	2 2
	Тематика практических занятий	6
	Установка операционной среды, настройка интерфейса операционной системы (рабочий стол, безопасность системы, подключение к сети). Установка прикладных программ. Управление файлами данных на локальных съемных запоминающих устройствах, а также на дисках локальной компьютерной сети, в Интернете	2 4
	Практическая подготовка	3
Тема 1.3. Диагностика неисправностей системы, ведение документации	Содержание	2
	Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	1 1
	Тематика практических занятий	2
	Диагностика простейших неисправностей персонального компьютера, периферийного оборудования и компьютерной оргтехники Оформление отчетной документации в соответствии с перечнем работ, выполняемых в порядке текущей эксплуатации ЭВМ	1 1
	Практическая подготовка	3
Раздел 2. Создание и управление на персональном компьютере текстовыми документами, таблицами, презентациями и		88

содержанием баз данных, работа в графических редакторах		
Тема 2.1. Работа в текстовом процессоре	Содержание	4
	Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре. Работа с таблицами, диаграммами, графическими объектами в текстовом процессоре.	2 1 1
	Тематика практических занятий	15
	Создание документов в текстовом процессоре, создание документов с помощью шаблонов, ввод текстовой информации, сохранение документов Форматирование и редактирование документов в текстовом процессоре. Работа с таблицами, диаграммами, графическими объектами в текстовом процессоре. Печать документов в текстовом процессоре. Сканирование текстовых документов и их распознавании.	1 6 6 2
	Практическая подготовка	20
Тема 2.2. Работа в редакторе электронных таблиц	Содержание	6
	Создание и форматирование таблицы в редакторе электронных таблиц Работа со встроенными функциями в электронной таблице Создание и работа с диаграммами и графиками	2 2 2
	Тематика практических занятий	20

	Создание и форматирование таблицы в редакторе электронных таблиц Вычисление с помощью формул в электронной таблице	4
	Работа со встроенными функциями в электронной таблице	4
	Работа со списками в электронной таблице Создание форм для ввода данных таблицы Создание и работа с диаграммами и графиками	2
	Обмен данными между текстовым процессором и электронной таблицей	2
		2
		4
		2
	Практическая подготовка	22
Тема 2.3. Работа в программе подготовки и просмотра презентаций	Содержание	5
	Построение презентации различными способами	3
	Обработка объектов слайдов презентации	2
	Тематика практических занятий	13
	Построение презентации различными способами Обработка объектов слайдов презентации Настройка анимации объектов	6
	Настройка показа и демонстрация результатов работы средствами мультимедиа	4
		2
		1
	Практическая подготовка	15
Тема 2.4. Работа в системе управления базами	Содержание	2
	Ввод данных в таблицы базы данных	2
	Тематика практических занятий	5

данных	Ввод данных в таблицы базы данных	2
	Создание простых запросов без параметров и с параметрами. Создание отчетов.	3
	Практическая подготовка	7
Тема 2.5. Работа в графических редакторах	Содержание	4
	Рисование объектов средствами графического редактора.	2
	Работа с эффектами в программе векторной графики.	2
	Тематика практических занятий	14
	Работа с заливками и контурами в программе векторной графики. Работа с текстом в программе векторной графики.	2
	Работа с эффектами в программе векторной графики.	2
	Вставка и редактирование готового изображения с использованием программ растровой графики.	2
	Работа с цветом с использованием программ растровой графики.	2
	Работа со слоями с использованием программ растровой графики.	2
	Работа со спецэффектами с использованием программ растровой графики.	2
	Практическая подготовка	16
Раздел 3. Использование ресурсов технологий и сервисов Интернета		14
Тема 3.1. Работа с ресурсами Интернета	Содержание	4
	Создание и обмен письмами электронной почты.	1
	Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера.	3
	Тематика практических занятий	10

	Создание и обмен письмами электронной почты. Навигация по Веб-ресурсам Интернета с помощью программы Веб-браузера. Поиск, сортировка и анализ информации с помощью поисковых Интернет-ресурсов. Пересылка и публикация файлов данных в Интернете.	2 3 3 2
	Практическая подготовка	10
Раздел 4. Обеспечение защиты информации в компьютерной системе		14
Тема 4.1. Защита информации при работе с офисными приложениями	Содержание	8
	Использование штатных средств защиты операционной системы и прикладных программ. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных, резервного копирования и восстановления данных	4 2 2
	Тематика практических занятий	11
	Использование штатных средств защиты операционной системы и прикладных программ. Применение парольной защиты. Установка антивирусных программ, их настройка. Обновление базы. Выполнение архивирования данных, резервного копирования и восстановления данных	4 1 3 3
	Практическая подготовка	12
Тематика самостоятельной учебной работы: проработка конспектов занятий, учебной и специальной литературы		4
Практическая подготовка		112
Промежуточная аттестация по учебной практике		оценка
Промежуточная аттестация по производственной практике		зачет с оценкой

Квалификационный экзамен	12
Всего	315

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Кабинет информатики и ИКТ, оснащенный оборудованием: компьютерные столы, компьютерные кресла, стулья на каждого обучающегося, конференц-стол, стол преподавателя, комплект учебно-наглядных пособий; дидактический раздаточный материал;техническими средствами: компьютеры, проектор, принтер, колонки, наушники, локальная сеть.

Оснащенные базы практики, в соответствии с п 6.2.3 Примерной программы по специальности 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе.

3.2.1. Печатные издания2

1. Богомазова Г.Н. Установка и обслуживание программного обеспечения персональных компьютеров, серверов, периферийных устройств и оборудования: учеб. для студ. учреждений сред. проф. образования /Г.Н. Богомазова. - М.: Издательский центр «Академия», 2015. - 256 с.

2. Михеева Е.В. Информационные технологии в профессиональной деятельности: учеб. пособие для студ.учреждений сред. проф.образования / Е.В.Михеева. - 14-е изд., стер. - М.: Издательский центр «Академия», 2016. - 384 с.

3. Струмпэ Н.В. Оператор ЭВМ. Практические работы: учеб. пособие для студ. учреждений сред. проф. образования / Н.В. Струмпэ. - 7-е изд., стер. - М.: Издательский центр «Академия», 2015. - 112 с.

3.2.2. Электронные издания (электронные ресурсы)

1. Федеральный образовательный портал. Библиотека. Единое окно доступа к образовательным ресурсам: http://window.edu.ru/library

2. Образовательная платформа Юрайт https://urait.ru

3. Информационныйресурс издательского центра«Академия» https://www.academia-moscow.ru/

3.2.3. Дополнительные источники

1. Максимов Н.В., Партыка Т.Л., Попов И.И. Архитектура ЭВМ и вычислительных систем: учебник /Н.В. Максимов, Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА-М, 2013 - 512 с.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1. Осуществлять подготовку оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	Демонстрировать умения и практические навыки в подготовке оборудования компьютерной системы к работе, производить инсталляцию, настройку и обслуживание программного обеспечения	тестирование, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнениявидов работ на практике
ПК 4.2 Создавать и управлять на персональном компьютере текстовыми документами, таблицами, презентациями и содержанием баз данных, работать в графических редакторах	Проявление умения и практического опыта в работе с текстовыми документами, таблицами и презентациями, а также базами данных	тестирование, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнениявидов работ на практике
ПК 4.3 Использовать ресурсы локальных вычислительных сетей, ресурсы технологий и сервисов Интернета	Умение пользоваться ресурсами локальных вычислительных сетей, осуществлять поиск, анализ и интерпретацию информации	тестирование, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения ситуационных задач, оценка процесса и результатов выполнениявидов работ на практике
ПК 4.4 Обеспечивать применение средств защиты информации в компьютерной системе	Применение средств защиты информации в компьютерной системе	тестирование, экзамен квалификационный, экспертное наблюдение выполнения практических работ, оценка решения

		ситуационных задач, оценка процесса и результатов выполнения видов работ на практике
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	- обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной практике Экзамен квалификационный
ОП 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, Медиа-ресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; обоснованность анализа работы членов команды (подчиненных)	

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;	
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно- коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	