

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

*Приложение к ОПОП
10.02.04 Обеспечение
информационной безопасности
телекоммуникационных систем*

РАБОЧИЕ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
к специальности 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Содержание:

1. ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей
2. ПМ.02 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты
3. ПМ.03 Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты
4. ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих (для специальностей СПО)

Шатура
2024

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

к 10.02.04 Обеспечение информационной безопасности
телекоммуникационных систем

Шатура
2024

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППСЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Еремина Елена Алексеевна, преподаватель специальных дисциплин

Аверьянов Алексей Станиславович, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС
Информатика и вычислительная техника и Информационная
безопасность (09.02.06, 10.02.04)

Протокол № ____ от « ____ » _____ 20 ____ г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Н.В. Еркина, методист ГБПОУ МО
«ШЭТ»

СОДЕРЖАНИЕ:

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ. 01. Эксплуатация информационно-телекоммуникационных систем и сетей

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен **ОСВОИТЬ** **ОСНОВНОЙ ВИД** деятельности эксплуатация информационно-телекоммуникационных систем и сетей и соответствующие ему общие и профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих 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.
ЛП 10	Заботящийся о защите окружающей среды, собственной и чужой безопасности, в том числе цифровой
ЛП 15	Проявляющий гражданское отношение к профессиональной деятельности как к возможности личного участия в решении общественных, государственных, общенациональных проблем
ЛП 17	Принимающий цели и задачи научно-технологического, экономического, информационного и социокультурного развития России, готовый работать на их достижение.
ЛП 19	Готовый к профессиональной конкуренции и конструктивной реакции на критику.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД1	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.

1.1.3. В результате освоения профессионального модуля студент должен:

Иметь практический опыт	- 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 приемопередающих устройств (1ШУ); - читать принципиальные схемы блоков 1ШУ; - выполнять расчеты, связанные с определением значений параметров режима и элементов 1111У; - контролировать работу и осуществлять техническую эксплуатацию 1111У;

	- 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

	- типовые услуги, предоставляемые с использованием информационно-телекоммуникационных сетей, виды информационного обслуживания, предоставляемые пользователям; - принципы построения и технические средства локальных сетей; - принципы функционирования маршрутизаторов; модемы, используемые 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 проверок 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 836 часов в том числе в форме практической подготовки 288 часов Из них:

на освоение МДК 01.01 214 часов

МДК 01.02 250 часов

МДК 01.03 76 часов

в том числе, самостоятельная работа 4 часа

курсовой проект - 30 часов

на практики, в том числе:

учебную - 144 часа производственную - 144 часа

Промежуточная аттестация - 24 часа, в том числе: дифференцированный зачеты и консультации - 16ч., экзамен по модулю -8 ч.

2. Структура и содержание профессионального модуля

2.1. Структура профессионального модуля

Коды профессиональн ых общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.						
			Работа обучающихся во взаимодействии с преподавателем						Самостоятельная работа
			Обучение по МДК			Практики		Консультации	
			Всего	В том числе		Учебная	Производ ственная		
				Лабораторных и практических занятий	Курсовых работ (проектов)				
1“ 1	2	3	5	6	7	9	10	11	12
ПК 1.1 -1.4 ОК 1-4, ОК 9,10 ЛР 10, 15, 17, 18	Раздел 1 .Приемо-передающие устройства, линейные сооружения связи и источники электропитания	214	206	96	-	-	-	8	-
ПК 1.1-1.4 ЛР 10, 15, 17, 18	Раздел 2.Телекоммуникационные системы и сети	250	240	120	-	-	-	8	2
ПК 1.1, 1.2, 1.4 ОК 1 -4 ОК9ДО ЛР 10, 15, 17, 18	Раздел 3. Электроизмерения и метрология	76	74	12	-	-	-	-	2
	Учебная практика	144	-	-	-	144	-	-	-
	Производственная практика (по профилю специальности)	144					144	-	-
	Промежуточная аттестация (экзамен по ПМ)	8	8	-	-	-	-	-	-
	Всего:	836	528	228	-	144	144	16	4

2.2. Тематический план и содержание профессионального модуля ПМ.01 Эксплуатация информационно-телекоммуникационных систем и сетей

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем в часах
1	2	3
Раздел 1. Приемо-передающие устройства, линейные сооружения связи и источники электропитания		214
МДК 01.01. Приемо-передающие устройства, линейные сооружения связи и источники электропитания		206
Подраздел 1. Технические средства и обслуживание передающего оборудования защищённых телекоммуникационных систем		54
Тема и. Назначение, структурная схема и технические характеристики радиопередатчика.	Содержание	2
	1. Определение и назначение радиопередающего устройства (РПУ). Обобщённая структурная схема передатчика и основные характеристики передатчика. Назначение основных каскадов РПУ.	
Тема 1.2. Автогенераторы	Содержание	4
	1. 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 автогенераторы.	Содержание	4
	1. Стабильность частоты АГ, методы ее повышения. Кварцевая стабилизация частоты АГ. Устройство и работа кварцевого резонатора. Схемы включения кварцевого резонатора в АГт. Коррекция частоты кварцевого АГ. Преимущества и недостатки кварцевой стабилизации частоты. Схема кварцевого транзисторного АГ.	

Тема 1.4. Формирование сигналов. Возбудители и синтезаторы частот.	Содержание	4
	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.	
Тема 1.5. Режимы и принципы построения генераторов с внешним возбуждением. Схемы генераторов с внешним возбуждением (ГВВ)	Содержание	4
	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	4
	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	4
	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	4
	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	4
	Понятие импульсной модуляции (ИМ). Виды ИМ и её особенности. Структурная схема передатчика с ИМ. Параметры и спектр сигнала при ИМ. Структурная схемы модуляторов ИМ. Внутримпульсная частотная модуляция.	
	В том числе, практических занятий и лабораторных работ	20
	Исследование влияния дестабилизирующих факторов на работу автогенератора.	

	Исследование генератора, управляемого напряжением, используемого в синтезаторах частот.	
	Исследование умножителя частоты	
	Исследование амплитудного модулятора	
	Исследование частотного модулятора	
Подраздел 2. Техническое обслуживание и оборудование <i>приемных устройств</i> телекоммуникационных систем		54
Тема 2.1. Теоретические основы радиоприема. Структурные схемы радиотрактов приёмников. Основные понятия и характеристики радиоприёмных устройств.	Содержание	4
	Назначение, основные характеристики радиоприёмных устройств (РПМУ). Структурная схема РПМУ прямого усиления. Структурная схема супергетеродинного РПМУ и её особенности.	
Тема 2.2. Входные цепи приёмных устройств. Особенности входных цепей различных частотных диапазонов	Содержание	4
	Назначение входной цепи, классификация и основные характеристики. Структура входной цепи (ВЦ). ВЦ с сосредоточенными и распределёнными элементами. Методика электрического расчёта вц.	
Тема 2.3. Резонансные усилители. Усилители радиочастоты. Маломощные усилители СВЧ	Содержание	4
	Назначение и основные характеристики резонансного усилителя. Структурная схема резонансного усилителя и режимы его работы. Маломощные усилители сверхвысокой частоты (СВЧ). Методика электрического расчёта усилителя СВЧ.	
Тема 2.4. Преобразователи частоты радиоприёмников. Виды преобразователей частоты	Содержание	4
	Назначение, структура и принцип работы преобразователя частоты (ПЧ). ПЧ с отдельным гетеродином. ПЧ с совмещённым гетеродином. Расчёт промежуточной частоты и преобразователя частоты.	
	Содержание	

Тема 2.5. Усилители промежуточной частоты радиоприёмных устройств	Назначение и схемотехника усилителя промежуточной частоты (УПЧ). Стандартные промежуточные частоты радиоприёмных устройств. Многокаскадные УПЧ. Избирательные элементы в УПЧ?	4
Тема 2.6. Детекторы сигналов. Амплитудное детектирование. Детекторы импульсных сигналов	Содержание	2
	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	2
	Амплитудные ограничители. Назначение, основные характеристики и принцип работы частотного детектора. Схемотехника частотных детекторов.	
Тема 2.8. Принцип работы фазовых детекторов. Виды фазовых детекторов	Содержание	2
	Назначение, принцип работы и основные характеристики фазового детектора (ФД). Искажения характеристики ФД. Схемотехника ФД.	
Тема 2.9. Регулировки в радиоприёмных устройствах	Содержание	2
	Регулировка усиления. Настройки радиоприемников. Регулировка полосы пропускания. Устройства индикации РПМУ.	
Тема 2.10. Автоматическая регулировка усиления	Содержание	2
	Назначение, параметры и принцип работы схем автоматической регулировки усиления (АРУ). Основные схемы АРУ.	
Тема 2.11. Автоподстройка частоты в радиоприёмных устройствах	Содержание	2
	Принцип автоматической подстройки частоты в радиоприёмных устройствах. Структурные схемы систем АПЧ различных видов, назначение каскадов. Основные характеристики системы АПЧ.	
Тема 2.12. Регулировка полосы пропускания	Содержание	2
	Способы регулировки полосы пропускания приёмника Особенности регулировок полосы пропускания в различных каскадах радиоприёмника.	

	В том числе, практических занятий и лабораторных работ	20
	Исследование резонансного усилителя радиочастоты	
	Исследование преобразователя частоты с отдельным гетеродином	
	Исследование усилителя промежуточной частоты	
	Исследование отдельных функциональных блоков систем радиосвязи	
	Исследование отдельных функциональных блоков систем радиосвязи	
Подраздел 3. Линии связи		64
Тема 3.1. Построение сетей электросвязи	Содержание	2
	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 зонных сетей связи. Построение местных сетей связи.	
Тема 3.2. Воздушные линии связи	Содержание	2
	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
	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
	Кабели телефонных сетей и сетей проводного вещания (ИВ). Конструкция и назначение кабелей ГПП; 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 ПР1П1М, МРМ, ПТПЖ, ТРП (ТРВ); станционных кабелей ТСВ.	
	В том числе, практических занятий и лабораторных работ	

	Кабели с витой парой UTP, STP	16
	Кабели ТПП	
	Кабели СТС	
	Кабели ПВ	
Тема 3.5. Кабели магистральных и зонавых сетей	Содержание	2
	Конструкция симметричных кабелей типов МКС, ЗК. коаксиальных кабелей МКТ-4, КМ-4,-75, КРК-75.	
	В том числе, практических занятий и лабораторных работ	8
	Симметричные кабели	
	Коаксиальные кабели	
Тема 3.6. Волоконно оптические линии связи	Содержание	2
	Основы передачи информации по волоконно-оптическим линиям связи (ВОЛС). Структура и компоненты линейного тракта ВОЛС. Характеристики оптических компонентов ВОЛС.	
	В том числе, практических занятий и лабораторных работ	4
	Волоконно-оптические линии связи	
Тема 3.7. Кабельная Подземная инфраструктура телефонной связи	Содержание	4
	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 связи	Содержание	2
	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	
	Содержание	

Тема 3.9. Монтаж кабелей связи и оконечных кабельных устройств местных телефонных сетей	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.	2
	В том числе, практических занятий и лабораторных работ	12
	Монтаж кабеля ТПП, МКС, ЗКП	
	Монтаж КРТП-10, БМ	
	Монтаж МТОК	
Тема 3.Ю.Устройства ввода кабелей в здания станций (УП, ОУП), телефонизируемые здания	Содержание	2
	Кроссирование кабелей в АТС. Назначение шахты. Кроссирование кабелей в абонентские пункты.	
Тема 3.П.Кабели под постоянным воздушным избыточным давлением	Содержание	2
	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		8
Тема 4.1.Электрические характеристики воздушных и кабельных линий связи	Содержание	2
	Первичные и вторичные параметры электрических кабелей и воздушных линий связи (ВЛС). Частотные диапазоны использования электрических кабелей и ВЛС	
Тема 4.2.Параметры волоконно-оптических линий	Содержание	2
	Параметры волоконно-оптических линий (ВОЛС).Критическая частота и длина волн волоконного световода. Типы волн в световоде. Затухание волоконных световодов. Дисперсия и пропускная способность световодов.	
	В том числе, практических занятий и лабораторных работ	4
	Измерение электрических характеристик симметричных кабелей	

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
	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
	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.	
Подраздел 6. Защита линий связи от влияния внешних источников и коррозии		12
Тема 6.1.Источники опасных и мешающих влияний. Меры защиты линейных сооружений связи	Содержание	2
	Основные понятия об источниках электромагнитного влияния на линии связи. Меры защиты линейных сооружений от опасного влияния атмосферного электричества, линий электропередачи, электрофицированного транспорта и радиостанций. Схемы защиты и элементы защиты. Оборудование заземлений.	
Тема 6.2.Защита сооружений связи от коррозии	Содержание	2
	Основные виды коррозии: почвенная, атмосферная, электролитическая, межкристаллитная. Их характеристика. Меры защиты от коррозии.	
	В том числе, практических занятий и лабораторных работ	8
	Исследование элементов защиты от внешних влияний	
	Измерения при защите кабеля от коррозии	
Подраздел 7.Техническое обслуживание линий связи		8
	Содержание	

Тема 7.1.Организация и осуществление технической эксплуатации линейных сооружений местных телефонных сетей	Организация эксплуатации. Задачи и методы технической эксплуатации. Охрана кабельных сооружений и аварийно-восстановительные работы. Электрические измерения в процессе эксплуатации.	2
Тема 7.2.Надежность линий связи	Содержание	2
	Обеспечение надежности линий связи. Показатели надежности. Оценка надежности и мероприятия по повышению надежности на линиях связи.	
	В том числе, практических занятий и лабораторных работ	4
	Исследование показателей надежности линий связи	
Консультации		8
Раздел 2. Телекоммуникационные системы и сети		250
МДК.01.02. Телекоммуникационные системы и сети		240
Тема 2.1 Изучение сети	Содержание	76
	Введение в сетевые технологии. Обзор компонентов сети Классификация компьютерных сетей Подключение к Интернету Сетевые стандарты. Протоколы. Эталонная модель OSI Модель TCP/IP Протокольный блок данных (PDU). Инкапсуляция. Сравнение моделей TCP/IP и OSI Стандарты Ethernet для проводных сетей Стандарты Ethernet для беспроводных сетей Сетевые устройства Кабели и разъемы Сетевая адресация Классовая и бесклассовая адресация IPv4 Форматы адресов IPv6 Статическая и динамическая адресация	50

	Протокол ICMP	
	Домен и рабочая группа	
	В том числе практических занятий и лабораторных работ	26
	Создание и тестирование сетевых кабелей.	
	Изучение сетевых инструментов совместной работы	
	Представление сети	
	Добавление компьютеров в существующую сеть.	
	Подключение к беспроводному маршрутизатору и настройка основных параметров	
	Подключение беспроводных компьютеров к беспроводному маршрутизатору.	
	Проверка беспроводного подключения.	
	Прокладка простой сети.	
	Подключение ПК к домену и рабочей группе.	
Тема 2.2 Настройка сетевой операционной системы	Содержание	28
	Cisco IOS. Способы доступа. Навигация по IOS. Структура команд Базовая настройка устройств Порты и адреса. Настройка IP.	16
	В том числе практических занятий и лабораторных работ	12
	Настройка начальных параметров коммутатора	
	Создание основных подключений	
	Отработка комплексных практических навыков базовой настройки сетевых устройств.	
Тема 2.3 Сетевые протоколы	Содержание	22
	Кодирование, размер, синхронизация сообщений	14
	Набор протоколов	
	Функции уровней OSI	
	Сегментация и мультиплексирование	
	Доступ к данным	
	В том числе практических занятий и лабораторных работ	8
	Изучение моделей TCP/IP и OSI в действии	
	Установка программы Wireshark. Просмотр сетевого трафика	
Тема 2.4 Сетевой доступ	Содержание	6
	Управление доступом к среде	2
	В том числе практических занятий и лабораторных работ	4
	Подключение проводных и беспроводных локальных сетей	
Тема 2.5 Ethernet	Содержание	12
	Кадр Ethernet	6

	Коммутаторы локальных сетей	
	Протокол разрешения адресов (ARP)	
	В том числе практических занятий и лабораторных работ	6
	Определение MAC- и IP-адресов	
Тема 2.6 Сетевой уровень	Изучение таблицы ARP	
	Содержание	22
	Характеристики протокола IP. Настройка маршрутизатора	2
	В том числе практических занятий и лабораторных работ	20
	Изучение межсетевых устройств	
	Настройка исходных параметров маршрутизатора	
	Подключение маршрутизатора к локальной сети	
	Устранение неполадок, связанных со шлюзом по умолчанию	
	Настройка базовых параметров маршрутизатора и коммутатора. Тестирование сквозного соединения.	
Тема 2.7 IP-адресация	Содержание	26
	Сетевые адреса. Проверка соединения.	8
	Проверка соединения. Трассировка маршрута. Разделение IP-сетей на подсети	
	В том числе практических занятий и лабораторных работ	16
	Анализ трафика одноадресной, широковещательной и многоадресной рассылки	
	Проверка адресации IPv4 и IPv6	
	Выполнение команды ping и трассировка маршрута для проверки пути	
	Устранение проблем с адресацией IPv4 и IPv6	
	Разработка схемы адресации. Проверка соединения.	
Тема 2.8 Концепция маршрутизации	Содержание	
	Характеристики сети	
	Механизмы пересылки пакетов	
	Концепция маршрутизации	
	Маршрутизация пакетов	
	Таблица маршрутизации	
	Операции маршрутизатора	
	Реализация статических маршрутов	
	Обзор динамических протоколов маршрутизации	
	В том числе практических занятий и лабораторных работ	10
	Исследование маршрутов с прямым подключением	
	Настройка статического маршрута	

	Настройка протокола RIPv2	
Тема 2.9 Коммутируемые сети	Содержание	
	Коммутируемые сети Способы пересылки на коммутаторе Домены коллизий Первоначальная настройка коммутатора Защищенный удаленный доступ Безопасность порта коммутатора	8
	В том числе практических занятий и лабораторных работ	8
	Настройка параметров коммутатора	
	Настройка параметров коммутатора	
	Настройка сетей VLAN	
	Конфигурация транковых каналов.	
Консультации		8
Самостоятельная работа		2
Раздел 3. Электрорадиоизмерения и метрология		74
МДК.01.03. Электроизмерения и метрология		74
Подраздел 1. Основы метрологии		20
Тема 1.1 .Наука об измерении, физические величины	Содержание	2
	Общие сведения о метрологии, стандартизации и сертификации. Метрология как наука об измерениях.	
Тема 1.2.Измерение физических величин	Содержание	4
	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	4
	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
	Общие сведения о теории измерений. Физические явления и эффекты, положенные в основу измерений. Методы измерений. Методика выполнения измерения.	
	Практическая работа № 1	2

	Физические величины и их единицы	
Тема 1.5. Основы теории погрешностей измерений	Содержание	2
	Общие сведения. Классификация погрешностей. Систематические погрешности. Случайные погрешности. Классы точности средств измерения.	
Тема 1.6. Обработка результатов измерений	Содержание	2
	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
	Цель и задачи государственной системы обеспечения единства измерений (ГСОЕИ). Законодательная база ГСОЕИ. Нормативная база ГСОЕИ. Метрологический надзор.	
Подраздел 2. Измерительные приборы		12
Тема 2.1. Принципы построения средств измерения	Содержание	2
	Обобщённая структурная схема измерительного прибора. Шкалы измерительных приборов, цена деления шкалы прибора.	
Тема 2.2. Аналоговые измерительные приборы	Содержание	4
	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	4
	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.	
	Практическая работа №2	2
	Измерение электрического сигнала аналоговыми и цифровыми приборами	
Подраздел 3. Источники электрических сигналов		8
Тема 3.1 .Измерительные генераторы	Содержание	2
	Назначение генераторов измерительных сигналов. Классификация генераторов. Схемы задающих генераторов. Установка частоты задающих генераторов.	
	Содержание	4

Тема 3.2. Основные типы генераторов сигналов	Генераторы гармонических колебаний. Цифровые измерительные генераторы низких частот. Генераторы шумовых сигналов, импульсные генераторы. Стандарт частоты, синтезаторы частоты. Органы управления генератором, выходные цепи генераторов.	
	Практическая работа №3	2
	Изучение работы генератора стандартных сигналов	
Подраздел 4. Методы и средства измерения параметров сигналов		10
Тема 4.1. Измерение параметров тока, напряжения и мощности сигналов	Содержание	2
	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
	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	4
	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.	
	Практическая работа №4	2
	Измерение параметров электрического сигнала с помощью электронного осциллографа	
Подраздел 5. Методы и средства измерения параметров компонентов радиотехнических цепей		6
Тема 5.1. Методы и средства измерения параметров компонентов радиотехнических цепей	Содержание	4
	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.	
	Практическая работа №5	2
	Измерение параметров электрического сигнала цифровыми приборами.	
Подраздел 6. Измерения в телекоммуникационных системах		12

Тема 6.1. Измерения в телекоммуникационных системах	Содержание	6
	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	4
	Структурная схема генератора шумовых сигналов. Структурная схема измерителя шума и вибраций. Структурная схема измерителя уровня. Цифровой вольтметр.	
	Практическая работа №6	2
	Изучение средств измерений для оценки защищённости конфиденциальной информации	
Подраздел 7. Основы технического регулирования		4
Тема 7.1 .Технические регламенты и стандарты.	Содержание	4
	Общие сведения. Закон РФ «О техническом регулировании». Технические регламенты.	
Тема 7.2. Сертификация продукции.	Подтверждение соответствия и сертификация. Принципы и формы подтверждения соответствия. Добровольная сертификация. Обязательная сертификация.	
	Дифференцированный зачет	2
Самостоятельная работа при изучении раздела ИМ		2
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.		
Учебная практика		144
Производственная практика		144
Экзамен по модулю		8
Всего		836

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть 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. Воробьев О. В. Приемно-передающие устройства, линейные сооружения связи и источники электропитания: учебное издание / Воробьев О. В., Глаголев С. Ф., Былина М. С. - Москва : Академия, 2024. - 288 с.

2. Костров Б. В. Сети и системы передачи информации: учебное издание / Костров Б. В., Ручкин В. Н. - Москва : Академия, 2024. - 288 с.

3. Никитин В. Е. Телекоммуникационные системы и сети: учебное издание / Никитин В. Е., Никитин М. Е., Утусиков С. В. - Москва : Академия, 2019. - 288 с.

4. Бубнов А. А. Техническая защита информации в объектах информационной инфраструктуры: учебное издание / Бубнов А. А., Пржегорлинский В. Н., Фомина К. Ю. - Москва : Академия, 2019. - 272 с.

3.2.2. Электронные издания (электронные ресурсы)

Ярочкина Г.В. Основы технических измерений (электроизмерения): ПУМ: учебное издание / Ярочкина Г.В. - Москва : Академия, 2021

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» <http://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, поиска неисправностей и ремонте оборудования ИТКС;	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, медиа ресурсы, 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, клиентами.	- 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

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

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

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Шатура
2024

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Краснолобов Дмитрий Михайлович, преподаватель специальных дисциплин
Еремина Елена Алексеевна, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС
Информатика и вычислительная техника и Информационная
безопасность (09.02.06, 10.02.04)

Протокол № ____ от «____» _____ 20____ г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Н.В. Еркина, методист ГБПОУ МО
«ШЭТ»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	4
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	8
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	24
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	32

**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 защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты и соответствующие ему профессиональные компетенции:

1.1.1 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.
ЛРЗ	Соблюдающий нормы правопорядка, следующий идеалам гражданского общества, обеспечения безопасности, прав и свобод граждан России. Лояльный к установкам и проявлениям представителей субкультур, отличающий их от групп с деструктивным и девиантным поведением. Демонстрирующий неприятие и предупреждающий социально опасное поведение окружающих

ЛР4	Проявляющий и демонстрирующий уважение к людям труда, осознающий ценность собственного труда. Стремящийся к формированию в сетевой среде личностно и профессионального конструктивного «цифрового следа»
ЛР7	Осознающий приоритетную ценность личности человека; уважающий собственную и чужую уникальность в различных ситуациях, во всех формах и видах деятельности.
ЛР14	Проявляющий сознательное отношение к непрерывному образованию как условию успешной профессиональной и общественной деятельности
ЛР19	Готовый к профессиональной конкуренции и конструктивной реакции на критику.

1.1.2 Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД1	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 систем и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты информации.

1.1.3 В результате освоения профессионального модуля студент

должен:

Иметь практический опыт	• 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 573 часов, в том числе в форме практической подготовки 563 часов. Из них:

на освоение МДК 02.01 215 часов;

МДК 02.02 98 часов;

в том числе, самостоятельная работа - 2 часа

курсовой проект - 30 часов

на практики, в том числе:

учебную - 108 часов

производственную - 144 часа

Промежуточная аттестация - 17 часов, в том числе:

экзамены, дифференцированные зачеты и консультации - 9 часов, экзамен по модулю - 8 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля.

Коды профессиональ ных общих компетенций	Наименования разделов профессионального модуля	Объем образовател ной программы, час.	Объем профессионального модуля, час.					Самостояте льная работа ¹
			Обучение по МДК			Практики		
			всего, часов	Лабораторн ых и практическ х занятий	Курсовы х работ (проекте в)*	Учебн ая	Произвол ственная	
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7,14,19	МДК 02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программноаппаратных средств защиты»	215	215	88	30	-	-	-
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7,14,19	МДК 02.02 «Криптографическая защита информации»	98	96	44	-	-	-	2
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7,14,19	Учебная практика	108	-	-	-	108	-	-

Примерная тематика самостоятельных работ в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием учебной дисциплины.

2.2. Тематический план и содержание профессионального модуля.

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
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»		573
МДК 02.01 «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты»		215
Тема 1.1. Обеспечение безопасности операционных систем	Содержание: • Проблемы обеспечения безопасности операционных систем. Полностью контролируемые системы. Частично-контролируемые системы. Windows 10. 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.	24

	- 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.	
	Практические и лабораторные работы	22
	Изучение средств идентификации аутентификации операционных систем Настройка локальной политики безопасности Windows. Политика паролей. Политики учетных записей. Назначение прав пользователя	4
	Настройка локальной политики безопасности Windows. Параметры безопасности. Политика аудита	4
	Настройка изолированной среды	2
	АПМДЗ Криптон-замок инициализация системного администратора, инициализация пользователя, проверка целостности среды	4
	Аппаратные средства шифрования Криптон4,8 настройка, эксплуатация	4
	Программные средства шифрования. Защищенные контейнеры. Криптон-шифрование	2
	Восстановление информации типовыми средствами Программы восстановления информации	2
Тема 1.2. Технологии разграничения доступа	Содержание:	30
	- 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. Инсталляция. 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 и лабораторные работы	16
	Программы надежного удаления информации	2

	Архивирование информации	4
	Программные средства резервного копирования. Настройка RAID-массивов	4
	Инсайдерская информация. Программы сбора информации о ПК	2
	Настройка межсетевого экрана.	4
Тема 1.3. Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN	Содержание:	20
	• 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 и лабораторные работы	42
	Основные действия с виртуальной машиной	4
	Работа с контрольными точками	4
	Использование внешних устройств	2
	Работа с локальным хранилищем сертификатов в ОС WINDOWS	2
	Установка и настройка ПО eTokenPKIClient	2
	Настройка ПО eTokenPKIClient с помощью групповых политик	2
	Развертывание TMS в среде Active Directory	2
	Настройка TMS в среде Active Directory	2
	Настройка политик TMS	4
	Настройка использования виртуального токена	2
	Использование токена на рабочем месте администратора	2
	Установка и настройка СКЗИ «КриптоПроС8Р»	2
	Работа с контейнерами закрытого ключа и сертификатами пользователя средствами Крипто Про CSP	2
	Применение SecretDisk4	2
	Применение SecretDisk Server NG	2
	Изучение основных возможностей ПО VipNetClient	2
	Изучение настроек ПО VipNetClient	2
	Изучение возможностей ПО Деловая почта	2
Тема 1.4. Технологии обнаружения вторжений	Содержание:	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 и лабораторные работы	8
	Изучение средств обнаружения атак	4
	Изучение антивирусных продуктов	4
Тема 1.5. Методы управления средствами защиты	Содержание:	8
	• 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.	
Курсовой проект (работа). Тематика курсовых проектов (работ): 1. Модель угроз НСД на предприятии. 2. Проведение классификации АС и СВТ по требованиям ФСТЭК на предприятии. 3. Проведение классификации ПО по требованиям ФСТЭК на предприятии. 4. Проведение классификации МЭ по требованиям ФСТЭК на предприятии. 5. Построение модели нарушителя по требованиям ФСТЭК на предприятии. 6. Построение модели нарушителя по требованиям ФСБ на предприятии. 7. Модель угроз безопасности ИС персональных данных на предприятии. 8. Комплексная модель защиты информации на предприятии. 9. Оценка эффективности существующих программных и программно-аппаратных средств защиты информации с применением специализированных инструментов и методов (индивидуальное задание). 10. Обзор и анализ современных программно-аппаратных средств защиты информации (индивидуальное задание). 11. Выбор оптимального средства защиты информации исходя из методических рекомендаций ФСТЭК и имеющихся исходных данных (индивидуальное задание). 12. Применение программно-аппаратных средств защиты информации от различных типов угроз на предприятии (индивидуальное задание). 13. Проблема защиты информации в облачных хранилищах данных и ЦОДах. 14. Защита сред виртуализации. 15. Анализ российского рынка средств обеспечения информационной безопасности беспроводных сетей. 16. Анализ зарубежного рынка средств обеспечения информационной безопасности беспроводных сетей. 17. Анализ методов и средств анализа защищенности беспроводных сетей. 18. Средства защиты акустической информации, современные проблемы и возможные (перспективные) пути их решения. 19. Виброакустические средства современных систем обеспечения информационной безопасности.		30

20. Средства защиты от ПЭМИН, современное состояние, проблемы и решения. 21. Средства обеспечения информационной безопасности проводных сетей общего доступа, методология и анализ применяемых решений. 22. Средства обеспечения информационной безопасности банков данных. 23. Разработка программы автоматизированного анализа результатов опросного метода оценки показателей обеспечения информационной безопасности деятельности организации, полученных методом сбора информации анкет (опроса). 24. Использование ЭЦП для обеспечения защиты информации при использовании системы электронного документооборота. 25. Обеспечение защиты конфиденциальной информации в распределённых системах разграничения доступа. 26. Анализ существующих методик оценки экономического ущерба от разглашения (утраты) конфиденциальной информации. 27. Информационная система мониторинга и координации деятельности сотрудников информационно-технического отдела. 28. Инструментальные средства анализа рисков информационной безопасности. 29. Сравнительный и оценочный анализ международных стандартов в области информационной безопасности и управления рисками. 30. Оценочный анализ методов и средств тестирования системы защиты вычислительных сетей (аудита информационной безопасности).		
Учебная практика раздела МДК 02.01. Виды работ: 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.		36
МДК 02.02 «Криптографическая защита информации»		98
Тема 2.1. Основы криптографических методов защиты информации	Содержание:	26
	• 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.	
	Практические и лабораторные работы	16
	Стеганографические методы скрытия информации	2
	Бинарная арифметика. Модульная арифметика	2
	Применение методов шифрования перестановкой	2
	Применение методов шифрования заменой	2
	Применение методов шифрования многоалфавитной замены	2
	Криптоанализ методов перестановки	2

Тема 2.2. Современные стандарты шифрования	Криптоанализ методов замены	2
	Компьютерное шифрование	2
	Содержание:	22
	• 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-Гамала. 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.	
	Практические и лабораторные работы	4
	Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа	2
	Асимметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители	2

Тема 2.3. Криптографические методы обеспечения безопасности сетевых технологий	Содержание: • Целостность сообщения. • Случайная модель Oracle. 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/MIME. • 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.	28
--	--	------------------

	• Защита информации в сетях сотовой связи. • А3. А8.А5/3. 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 и лабораторные работы	24
	Разработка хэш-функции	2
	Разработка схемы простого пароля	2
	Разработка схемы динамического пароля	2
	Сертификаты открытого ключа	2
	Настройка и администрирование токена	2
	Настройка сервисов Рутокен-PinPad	2
	Настройка сервисов Рутокен-ЭЦП	2
	Настройка сервисов Рутокен-Bluetooth	2
	Настройка сервисов Рутокен-S	2
	Разработка алгоритма PGP	2
	Изучение протоколов SSL, TLS, IPSec	2
	Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2	2

Самостоятельная учебная работа при изучении раздела МДК 02.02. Рекомендуемая тематика внеаудиторной (самостоятельной) работы: • Статистика и анализ крупных утечек информации за год. • Поиск информации о новых видах атак на информационную систему. • Обзор современных программных и программно-аппаратных средств защиты.	2
Учебная практика раздела МДК 02.02. Виды работ: • Проведение инструктажа по технике безопасности. Составление алгоритма хеш-функции. • Составление алгоритма шифра. • Подключение, установка драйверов, настройка программных средств шифрования Криптон. • Администрирование программных средств шифрования Криптон • Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон. • Администрирование аппаратных средств шифрования Криптон.	72
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.	144

• Подключение, установка драйверов, настройка программных средств абонентского шифрования. • Администрирование внедренных средств. • Настройка средств электронной подписи. • Администрирование средств электронной подписи. • Администрирование средств РКІ.	
Промежуточная аттестация	8
Всего	573

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы профессионального модуля требует наличия учебных кабинетов, лабораторий:

1. 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. Заводцев И. В. Программные и программно-аппаратные средства защиты информации в объектах информационной инфраструктуры: учебное издание /

Заводцев И. В., Крупенин А. В., Скрыль С. В. - Москва : Академия, 2023. - 320 с.

2. Ильин М. Е. Криптографическая защита информации в объектах информационной инфраструктуры: учебное издание / Ильин М. Е., Калинкина Т. И., Пржегорлинский В. Н. - Москва : Академия, 2024. - 288 с.

3. Костров Б. В. Сети и системы передачи информации: учебное издание / Костров Б. В., Ручкин В. Н. - Москва : Академия, 2024. - 288 с.

3.2.2. Электронные издания (электронные ресурсы):

Интернет-ресурсы:

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

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

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

4. Федеральный портал «Информационно- коммуникационные технологии в образовании» [httpW: www.ict.edu.ru](http://www.ict.edu.ru).

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

3.2.3. Дополнительные источники:

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

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

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

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

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

6. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».
7. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».
8. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».
9. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.
10. Положение о сертификации средств защиты информации по требованиям безопасности информации (с дополнениями в соответствии с постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации»). Утверждено приказом председателя Гостехкомиссии России от 27 октября 1995 г. № 199.
11. Положение по аттестации объектов информатизации по требованиям безопасности информации. Утверждено Гостехкомиссией России 25 ноября 1994 г.
12. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.
13. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.
14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 83.
15. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

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

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

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

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

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

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

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

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

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

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

26. ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология.

Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети

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

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

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

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

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

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

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

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

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

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

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

38. ГОСТ Р 56103-2014 Защита информации. Автоматизированные системы

в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Госстандарт, 2014.

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

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

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

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

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

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

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

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

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

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1 Контроль и оценка результатов освоения профессионального модуля.

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1 - 2.3 ОК 1-10 ЛР 3, 4, 7,14,19	«отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко; «хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками; «удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки; «неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Экспертная оценка результатов деятельности обучающихся в процессе освоения образовательной программы: - на практических занятиях (при решении ситуационных задач, при участии в деловых играх: при подготовке и участии в семинарах, при подготовке рефератов, докладов ит.д.); - при выполнении и защите курсовой работы (проекта); - при выполнении работ на различных этапах производственной практики; - при проведении: контрольных работ, зачетов, экзаменов по междисциплинарным курсам, экзамена (квалификационного) по модулю.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Шатура
2024

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Краснолобов Дмитрий Михайлович, преподаватель специальных дисциплин

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС
Информатика и вычислительная техника и Информационная
безопасность (09.02.06, 10.02.04)

Протокол № ____ от « ____ » _____ 20 ____ г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Н.В. Еркина, методист ГБПОУ МО
«ШЭТ»

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРИМЕРНОЙ 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
ВДЗ	Защита информации в информационно-телекоммуникационных системах и сетях с использованием технических и физических средств защиты
ПК3.1.	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
ПК3.3.	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.

ОК3.	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 практический опыт	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 не-санкционированной 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: **442 часа.**

Из них на освоение МДК **436 часов:**

МДК.03.01 Защита информации в ИТКС с использованием технических средств защиты-**141 час;**

МДК.03.02 Физическая защита линий связи ИТКС -**120 часов.**

На практики учебную и производственную -**175 часов.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Коды профес- сиональных общих компе- тенций	Наименования разделов профессионального мо- дуля	Объем об- разова- тельной программы, час.	Объем профессионального модуля, час.					Самостоя- тельная работа ¹	Консульта- ции
			Обучение по МДК			Практики			
			всего, часов	Лаборатор- ных и прак- тических занятий	Курсовых работ (проек- тов)*	Учеб- ная	Произ- вод- ствен- ная		
ПК3.1-ПК.3.4 ОК1 - ОК7, ОК 9 ЛР 3, 4, 7, 14, 19	Раздел 1. Защита инфор- мации в информационно- телекоммуникационных системах и сетях с исполь- зованием технических средств защиты	203	194	92	-	-	-	4	5
ПК 3.5 ОК1 - ОК7, ОК 9 ЛР 3, 4, 7, 14, 19	Раздел 2. Физическая за- щита линий связи инфор- мационно-телекоммуника- ционных систем и сетей	143	138	68	-	-	-	2	3
ПК3 1 -3.5 ОК 1- 10 ЛР 3, 4, 7, 14, 19	Учебная практика	108	-	-	-	108	-	-	-
ПК3. 1 -3.5 ОК 1- 10 ЛР 3, 4, 7, 14, 19	Производственная практика	72	-	-	-	-	72	-	-
	Промежуточная аттестация	8	8	-	-	-	-	-	-
	Всего:	534	340	160	-	108	72	6	8

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		203
МДК.03.01.Защита информации в ИТКС с использованием технических средств защиты		194
Тема 1.1. Предмет и задачи технической защиты информации	Содержание	2
	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	2
	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	2
	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 и лабораторные работы	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
	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 и лабораторные работы	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	4
Тема 2.3. Методы и средства технической разведки	Содержание	2
	Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.	
	Тематика практических занятий и лабораторных работ	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 3.1. Физические основы утечки информации по каналам побочных электромагнитных излучений и наводок	Содержание	2
	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	
	Тематика практических занятий и лабораторных работ	4
	Измерение параметров физических полей	4
Тема 3.2. Физические процессы при подавлении опасных сигналов	Содержание	2
	Скрытие речевой информации в каналах связи. Подавление опасных сигналов акустоэлектрических преобразований. Экранирование. Зашумление.	
	Практические и лабораторные работы	4

	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.1. Системы защиты от утечки информации по акустическому каналу	Содержание	2
	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 и лабораторные работы	4
	Защита от утечки по акустическому каналу	
Тема 4.2. Системы защиты от утечки информации по проводному каналу	Содержание	2
	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 и лабораторные работы	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.3. Системы защиты от утечки информации по вибрационному каналу	Содержание	2
	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 и лабораторные работы	4
	Защита от утечки по виброакустическому каналу	
Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу	Содержание	2
	Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу.	

	Практические и лабораторные работы	8
	Определение каналов утечки ПЭМИН	
	Защита от утечки по цепям электропитания и заземления	
Тема 4.5. Системы защиты от утечки информации по телефонному каналу	Содержание	2
	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 и лабораторные работы	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.6. Системы защиты от утечки информации по электросетевому каналу	Содержание	4
	Низкочастотное устройство съема информации. Высокочастотное устройство съема информации. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электросетевому каналу.	
	Практические и лабораторные работы	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 4.7. Системы защиты от утечки информации по оптическому каналу	Содержание	2
	Телевизионные системы наблюдения. Приборы ночного видения. Системы защиты информации по оптическому каналу.	
	Практические и лабораторные работы	2
	Тематика учебных занятий формируется образовательной организацией самостоятельно	
Тема 5.1. Применение технических средств защиты информации	Содержание	4
	Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромаг-	

	нитных 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.	
	Практические и лабораторные работы	10
	Тематика учебных занятий формируется образовательной организацией самостоятельно	10
Тема 5.2. Эксплуатация технических средств защиты информации	Содержание	4
	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 и лабораторные работы	16
	Тематика учебных занятий формируется образовательной организацией самостоятельно	16
Самостоятельная учебная работа при изучении раздела 1 ПМ		4
Рекомендуемая 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		143
МДК.03.02. Физическая защита линий связи ИТКС		138
Тема 1.1. Цели и задачи физической защиты объектов информатизации	Содержание	2
	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 и лабораторные работы	4
	Тематика учебных занятий формируется образовательной организацией самостоятельно	4
Тема 1.2. Общие сведения о комплексах инженерно-технических средств физической защиты	Содержание	3
	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 и лабораторные работы	12
	Тематика учебных занятий формируется образовательной организацией самостоятельно	12
Тема 2.1. Система обнаружения комплекса инженерно-технических средств физической защиты	Содержание	2
	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 и лабораторные работы	8
	Монтаж датчиков пожарной и охранной сигнализации	8
	Содержание	2

Тема 2.2. Система контроля и управления доступом	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 и лабораторные работы	6
	Рассмотрение принципов устройства, работы и применения аппаратных средств аутентификации пользователя	6
	Рассмотрение принципов устройства, работы и применения средств контроля доступа	
Тема 2.3. Система телевизионного наблюдения	Содержание	2
	Аналоговые и цифровые системы видеонаблюдения. Назначение системы телевизионного наблюдения. Состав системы телевизионного наблюдения. Видеокамеры. Объективы. Термокожухи. Поворотные системы. Инфракрасные осветители. Детекторы движения.	
	Практические и лабораторные работы	6
	Рассмотрение принципов устройства, работы и применения средств видеонаблюдения.	6
Тема 2.4. Система сбора, обработки, отображения и документирования информации	Содержание	2
	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 и лабораторные работы	2
	Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.	2
Тема 2.5. Система воздействия	Содержание	2
	Назначение и классификация технических средств воздействия. Основные показатели технических средств воздействия.	
	Практические и лабораторные работы	6

	Тематика учебных занятий формируется образовательной организацией самостоятельно	6
Тема 3.1. Применение инженерно-технических средств физической защиты	Содержание	2
	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.	
	Практические и лабораторные работы	14
	Тематика учебных занятий формируется образовательной организацией самостоятельно	14
Тема 3.2. Эксплуатация инженерно-технических средств физической защиты	Содержание	2
	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.	
	Практические и лабораторные работы	
	Тематика учебных занятий формируется образовательной организацией самостоятельно	12
Самостоятельная учебная работа при изучении раздела модуля 2		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.		
Учебная практика по профессиональному модулю		
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 шумления. 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.	100
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.	
Промежуточная аттестация (экзамен по модулю)	8
Всего по ПМ	534

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Лаборатория «Защиты информации от утечки по техническим каналам».

Оборудование мастерской:

- рабочее место преподавателя;
- посадочные места обучающихся (по количеству обучающихся);
- учебные наглядные пособия (таблицы, плакаты);
- тематические папки дидактических материалов;
- комплект учебно-методической документации;
- комплект учебников (учебных пособий) по количеству обучающихся.

Технические средства обучения:

- персональный компьютер с лицензионным программным обеспечением;
- мультимедиа проектор (проектор, экран);
- Маркерная доска;
- Программное обеспечение общего и профессионального назначения.

3.2. Информационное обеспечение обучения

Основные источники:

1. Пржегорлинский В. Н. Физическая защита информации в объектах информационной инфраструктуры: учебное издание / Пржегорлинский В. Н., Бубнов А. А., Фомина К. Ю. - Москва : Академия, 2024. - 192 с
2. Бубнов А. А. Техническая защита информации в объектах информационной инфраструктуры: учебное издание / Бубнов А. А., Пржегорлинский В. Н., Фомина К. Ю. - Москва : Академия, 2019. - 272 с
3. Технические средства автоматизации и управления: Учебное пособие/ Шишов О. В. - М.: НИЦ ИНФРА-М, 2020. - 396 с.: 60х90 1/16. - (Высшее образование: Бакалавриат) (Переплёт) ISBN 978-5-16-010325-9 <https://znanium.com/read?id=361160>

Дополнительные источники:

1. Технические средства автоматизации и управления: Учебное пособие / Шишов О. В. - М.: НИЦ ИНФРА-М, 2020. - 396 с.: 60х90 1/16. - ISBN 978-5-16-010325-9 <https://znanium.com/read?idA361160>
2. Бондарев П.В. Физическая защита ядерных объектов: Учебное пособие П.В. Бондарев, А.В. Измайлов, А.И. Толстой; Под ред. Н.С. Погожина. - М.: МИФИ, 2022. - 584 с.20
3. Козинный, А. Сейсмические средства обнаружения для охраны территориально

распределенных объектов / А. Козинный, А. Косарев, В. Матвеев // БДИ, 2021. № 4. С. 74-77.

4. Груба И. И. Системы охранной сигнализации. Технические средства обнаружения. —М.: СОЛОН-ПРЕСС, 2022. — 220 с

5. Зенов, А. Ю. Концепция организации обработки информации в системах диагностики и распознавания / А. Ю. Зенов, М. П. Берестень // Инженерный вестник Дона: электрон, научи, жури. 2023. №1. [Электронный ресурс]. -URL: <http://ivdon.ru/magazine/archive/nly2013/1568>

6. Гагарина, Лариса Геннадьевна. Технические средства информатизации: Учебное пособие. - 1. - Москва: Издательский Дом "ФОРУМ" : ООО "Научно-издательский центр ИНФРА-М", 2022. - 256 с. - ISBN 978-5-8199-0734-4 <http://znanium.com/go.php?id=1021128>

- Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 18.03.2019) «Об информации, информационных технологиях и о защите информации».

- Федеральный закон от 27 июля 2006 г. № 152-ФЗ (редакция, действующая с 1 марта 2021 года) «О персональных данных».

- Закон РФ "О государственной тайне" от 21.07.1993 N 5485-1 (с изменениями на 9 марта 2021 года)

- Федеральный закон "О коммерческой тайне" от 29.07.2004 N 98-ФЗ (с изменениями на 9 марта 2021 года)

- Доктрина информационной безопасности Российской Федерации 1

- Положение «О государственной системе защиты информации в российской федерации от иностранных технических разведок

- и от ее утечки по техническим каналам» (извлечения). Утверждено Постановлением Совета Министров - Правительства Российской

- Федерации от 15.09.1993 № 912-51.

- Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации»

- Федерального закона от 26 июля 2017 г. N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"

- Указ Президента Российской Федерации от 22 декабря 2017 года № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

- Федеральный закон от 27 декабря 2002 г. № 184-ФЗ (с изменениями на 22 декабря 2020 года) «О техническом регулировании».

- Федеральный закон от 4 мая 2011 г. № 99-ФЗ (с изменениями на 31 июля 2020

года) «О лицензировании отдельных видов деятельности».

- Федеральный закон от 30.12. 2001 № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях» (с изменениями на 9 марта 2021 года) (редакция, действующая с 27 марта 2021 года).

- Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю» (с изменениями на 31 августа 2020 года).

- Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера» (с изменениями на 13 июля 2015 года).

- 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. Постановление Правительства Российской Федерации от 26.06.1995 № 608.

- 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. № 21.22

- 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.

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

Электронные издания (электронные ресурсы):

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

- Федеральный портал «Информационно - коммуникационные технологии в образовании» <http://oso.rcsz.ru/info/kompas/edu.htm>
- Всероссийский образовательный портал <https://edu-ikt.ru/>
- www.dedal.ru.

- www.neurophotonica.ru.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Код и наименование профессиональных и общих компетенции, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК3.1. 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 ИТКС.	- проводить установку, монтаж, настройку и испытание технических средств защиты информации от утечки по техническим каналам; - проводить техническое обслуживание, устранение неисправностей и ремонт технических средств защиты информации от утечки по техническим каналам; - применять нормативные правовые акты и нормативные методические документы в области защиты информации;	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 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, клиентами.	- 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

		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. <i>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</i>
--	--	---

		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. <i>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</i>
--	--	---

ПК ^Обеспечивать применение средств защиты информации в компьютерной системе		Оценка выполнения и защиты практических работ; Оценка дифференцированного зачета по практике. Демонстрационный экзамен по модулю. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
---	--	--

МИНИСТЕРСТВО ОБРАЗОВАНИЯ МОСКОВСКОЙ ОБЛАСТИ
государственное бюджетное профессиональное
образовательное учреждение Московской области
«Шатурский энергетический техникум»
(ГБПОУ МО «ШЭТ»)

РАБОЧАЯ ПРОГРАММА

ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.04 Выполнение работ по одной или нескольким профессиям рабочих,
должностям служащих (для специальностей СПО)

10.02.04 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

г. Шатура
2024 г.

Рабочая программа учебной дисциплины разработана в соответствии Федеральным государственным образовательным стандартом (далее - ФГОС) по специальности программы подготовки специалистов среднего звена (далее ППССЗ) 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем (базовой подготовки).

Организация-разработчик: ГБПОУ МО «ШЭТ»

Разработчики:

Аверьянов Алексей Станиславович, мастер производственного обучения

ОДОБРЕНО

цикловой комиссией преподавателей специальности УГС
Информатика и вычислительная техника и Информационная
безопасность (09.02.06, 10.02.04)

Протокол № ____ от « ____ » _____ 20 ____ г.

Председатель ЦК: _____ Е.А. Еремина

Внутренний рецензент: _____ Н.В. Еркина, методист ГБПОУ МО
«ШЭТ»

СОДЕРЖАНИЕ

1 ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ	4
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	
2 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО	5
МОДУЛЯ	
3 СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО 6 МОДУЛЯ	
4 . УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО	21
МОДУЛЯ	

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ИМ. 04 ВЫПОЛНЕНИЕ РАБОТ ПО ОДНОЙ ИЛИ НЕСКОЛЬКИМ ПРОФЕССИЯМ РАБОЧИХ, ДОЛЖНОСТЯМ СЛУЖАЩИХ

1.1. Область применения программы

Рабочая программа профессионального модуля **ИМ. 04 Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих** (по профессии 14601 Монтажник оборудования связи) является частью основной профессиональной образовательной программы базовой подготовки 1П1ССЗ в соответствии с ФГОС по специальности СПО 10.02.04 Обеспечение информационной безопасности телекоммуникационных систем в части освоения основного вида профессиональной деятельности (ВПД): **Выполнение работ по одной или нескольким профессиям рабочих, должностям служащих** и соответствующих профессиональных компетенций (ПК):

ПК 4.1. Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно-телекоммуникационных систем и сетей

1.2. Цели и задачи модуля - требования к результатам освоения 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:

1.2.1. Перечень общих 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 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности

ОК 09. Использовать информационные технологии в профессиональной деятельности

ОК 10. Пользоваться профессиональной документацией на государственном и иностранных языках.

1.2.2. Перечень профессиональных компетенций

Код	Наименование результата обучения
ПК 4.1	Производить монтаж, настройку, проверку функционирования и конфигурирование оборудования информационно телекоммуникационных систем и сетей

1.2.3. В результате освоения профессионального модуля студент должен:

иметь практический опыт:

- Ознакомление с документацией по монтажу телекоммуникационного оборудования;
- Проверка телекоммуникационного оборудования и (или) его составных частей на соответствие документам и монтажной схеме;
- Сортировка оборудования, модулей и узлов, крепежных изделий;
- Подготовка инструментов и оборудования, необходимых для монтажа телекоммуникационного оборудования;
- Подготовка рабочего места к монтажу телекоммуникационного оборудования;
- Монтажа медно-жильных и волоконно-оптических кабелей связи.

уметь:

- выбирать вид кабеля для монтажа;
- выбирать и применять материалы и инструменты для монтажа медно-жильных и оптических кабелей связи;
- проводить работы по монтажу медно-жильных и оптических кабелей связи;
- соблюдать технологию запайки муфты (технологическую последовательность, дефекты, меры предупреждения и способы устранения);
- выполнять монтаж и заземление телекоммуникационного оборудования.

знать:

- виды медно-жильных и волоконно-оптических кабелей и их назначение;
- материалы и инструменты для монтажа медно-жильных и волоконно-оптических кабелей связи;
- порядок проведения работ по монтажу медно-жильных и волоконно-оптических кабелей связи;
- технологию запайки муфты;
- основные виды крепления деталей монтируемого оборудования связи и станционных кабелей;
- основы электротехники;
- простые электрические и монтажные схемы;

- назначение и устройство применяемых электроизмерительных приборов, правила пользования ими;
- устройство электрифицированного инструмента и механизмов;
- требования безопасности труда и пожарной безопасности на рабочем месте.

1.3. Количество часов, отводимое на освоение профессионального модуля

Всего часов - 228 часов;

из них на освоение МДК - 75 часов;

на практики -144 часа;

в том числе

учебную - 108 часов;

производственную - 36 часов

промежуточная аттестация - экзамен по модулю 8 ч.

Консультации 1 час.

2. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, 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	2	3	4	5	6	7	8	9
ОК 01 - ОК 10, ПК 4.1 - ПК 4.2	МДК 04.01 Монтажник оборудования связи	75	75	36				2
	УП 04. Учебная практика	108				108		
	1111 04. Производственная практика (по профилю специальности)	36					36	
	Консультации	1	1					
	Промежуточная аттестация - квалификационный экзамен	8	8					
	Всего:	228	84	36	-	108	36	2

2.2. Содержание обучения по профессиональному модулю (ПМ)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Тема 1.1 Технология электромонтажных работ	Содержание	16
	Оконцевание одножильных и многожильных проводов	6
	Контактные соединения одножильных и многожильных проводов скруткой	
	Ответвление одножильных и многожильных проводов	
	Сборка и проверка электрических схем	
	Практических занятия и лабораторные работы	10
	Снятие изоляции с провода. Зачистка жилы провода.	
	Зачистка жил проводов. Сращивание одножильных проводов	
	Зарядка элементов осветительной арматуры по принципиальной электрической схеме	
Тема 1.2 Монтаж контактных соединений	Содержание	20
	Лужение и пайка проводов.	10
	Контактные соединения пайкой	
	Пайка геометрических фигур	
	Практических занятия и лабораторные работы	10
	Зачистка жил проводов по заданным размерам	
	Лужение и пайка проводов.	
Тема 1.3 Монтаж симметричных кабелей связи	Содержание	20
	Монтаж коммутационных шнуров.	10
	Монтаж телекоммуникационных розеток категории 5е и 6.	
	Тестирование кабельной линии.	
	Практических занятия и лабораторные работы	10
	Изготовление патч-кордов 5 и 6 категории с помощью конвекторов и защитных колпачков	
	Проведение проверки патч-кордов лан тестером.	
	Фиксация кабелей нейлоновыми стяжками к основанию розетки	
	Содержание	16

Тема 1.4 Монтаж оконечных устройств	Сварка оптического волокна	10
	Монтаж оптических муфт МОГ, МТОК, МОГ-СПЛИТ, 2179-CS	
	Монтаж настенного оптического кросса	
	Практических занятия и лабораторные работы	6
	Снятие защитного покрытия с концов сращиваемых оптических волокон.	
	Сварка оптического волокна.	
	Сборка муфты. Демонтаж.	
Учебная практики		108
Виды работ		
Снятие изоляции с провода. Зачистка жилы провода.		
Скрутка жил провода по диаметру крепящего винта.		
Сращивание одножильных проводов.		
Ответвление одножильных и многожильных проводов.		
Зарядка элементов осветительной арматуры по принципиальной электрической схеме. Проверка правильности сборки схемы		
Лужение и пайка жил проводов.		
Соединения жил проводов пайкой. Контактные соединения пайкой		
Монтаж коммутационных шнуров.		
Монтаж телекоммуникационных розеток категории 5е иб.		
Тестирование кабельной линии.		
Сварка оптического волокна		
Укладка сваренных волокон в кассету		
Монтаж оптический муфты МОГ		
Монтаж настенного оптического кросса		
		36
Производственная практики (по профилю специальности) Виды работ		
Разделка сердечника кабеля ТППЭп на пучки, прозвонка Сращивание жил кабеля ТППЭп в одну гильзу, про звонка Сращивание жил кабеля ТППЭп в две гильзы, про звонка Устранение повреждений КРТМ «KRONE». Прозвонка. Нахождение и устранение повреждений в БКТО 200х2 Тестирование кабельной линии.		
Монтаж оптических муфт		
Монтаж настенного оптического кросса		
	Консультации	1

	Самостоятельная работа	2
	Промежуточная аттестация - экзамен	8
	ВСЕГО	228

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.2. Требования к минимальному материально-техническому обеспечению

Оборудование рабочих мест мастерской «Монтаж кабеля»:

- комплект антистатической мебели по количеству обучающихся, в составе стол 700x1200, светильник флуоресцентный, электромонтажная панель на 6 розеток, кресло;
- комплект специализированного оборудования для оснащения мастерской;
- комплект мебели для оснащения мастерской в составе верстак универсальный, шкаф для инструментов, стеллаж универсальный;
- автоматизированное рабочее место (АРМ) преподавателя, в составе персональный компьютер, МФУ принтер, проектор, экран;
- оборудование для рабочего места кабельщика-спайщика;
- комплект инструментов для разделки оптического кабеля НМ-1;
- заготовки;
- комплект учебно-методической документации (инструкционно-технологические карты);
- методические указания по выполнению самостоятельных работ;
- наглядные пособия (информационные стенды, планшеты по монтажу кабеля), в том числе плакаты, схемы.

2. Оборудование лаборатории и рабочих мест лаборатории «Монтаж кабеля»:

- комплект лабораторной антистатической мебели по количеству обучающихся;
- рабочее место преподавателя, оснащенное комплектом специализированного оборудования;
- технологическая оснастка;
- наборы инструментов;
- заготовки;
- комплект учебно-методической документации (инструкционно-технологические карты);
- методические указания по выполнению самостоятельных работ;
- наглядные пособия (информационные стенды, планшеты по монтажу кабеля), в том числе плакаты, схемы.

Технические средства обучения:

- видеозвукозаписывающая и воспроизводящая аппаратура;
- компьютер с лицензионным программным обеспечением;

2. Оборудование лаборатории и рабочих мест лаборатории «Структурированные кабельные системы»:

- комплект лабораторной антистатической мебели по количеству обучающихся;
- рабочее место преподавателя, оснащенное комплектом специализированного оборудования;
- технологическая оснастка;
- наборы инструментов;
- заготовки;
- комплект учебно-методической документации (инструкционно-технологические карты);
- методические указания по выполнению самостоятельных работ;
- наглядные пособия (информационные стенды, планшеты по монтажу кабеля), в том числе плакаты, схем;
- стенд для изучения оптико-волоконных систем передачи данных.

Технические средства обучения:

- видеозвукозаписывающая и воспроизводящая аппаратура;
- компьютер с лицензионным программным обеспечением;
- комплект мультимедийного и вспомогательного оборудования

- комплект мультимедийного и вспомогательного оборудования.

4. Оборудование полигона и рабочих мест полигона:

- рабочее место преподавателя;
- рабочие места учащихся оснащенные консолями для монтажа кабеля и муфт;
- комплект инструмента кабельщика-спайщика;
- комплект инструмента «НИМ»;
- строительный термофен;
- материалы для герметизации муфт;
- материалы для монтажа кабеля;
- наглядные пособия (информационные стенды, плакаты, макеты «монтаж различных муфт»).

Оснащенная база практики:

Оборудование и технологическое оснащение рабочих мест:

- основное электрооборудование электрических станций и сетей;
- воздушные и кабельные линии электропередачи распределительных сетей;
- такелажная оснастка для подъема и перемещения узлов и деталей оборудования;
- установки для прокладки и установки муфт силовых кабелей

3.2. Информационное обеспечение реализации и 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. Портнов Э.Л. Принципы построения первичных сетей и оптических кабелей линий связи. Учебное пособие для вузов:-М.:Горячая линия-Телеком, 2021.

2. Никулин В.И. Теория электрических цепей: Учебное пособие / В.И. Никулин. - М.: ИЦ РИОР: НИЦ Инфра-М, 2015 - 240 с.

3. Гагарина, Л.Г. Введение в инфокоммуникационные технологии: Учебное пособие / Л.Г. Гагарина, А.М. Баин и др.; Под ред. д.т.н., проф. Л.Г.Гагариной - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2024 - 339 с.

Дополнительная литература:

1. Г.Г. Раннев, В.А. Сурогина, А.П. Тарасенко, И.В. Кулибаба, Физические основы получения информации : учебник / — 2-е изд., перераб. и доп. — М.: КУРС: ИНФРА-М, 2023 — 304 с.;

Интернет-ресурс:

1. <http://www.twipx.com>
2. <http://www.ssd.ru/>
3. <http://www.izmer-ls.ru/>

3.2.2. Общие требования к организации учебной практики

Учебная практика проводится на базе образовательного учреждения в мастерской «Мастерская по монтажу кабеля» и учебных лабораториях «Монтаж кабеля», «Структурированные кабельные системы».

Для выполнения программы учебной практики занятия рекомендуется проводить при делении группы на две подгруппы, что способствует повышению качества и

индивидуализации обучения. Проведение занятий учебной практики в подгруппах осуществляет мастер производственного обучения.

В учебном процессе используются информационные технологии обучения. Студенты обеспечены учебниками, инструкционно-технологическими картами и наглядными пособиями.

Результатом освоения программы учебной практики является квалификационный экзамен по результатам практики, проводимый в учебном заведении после ее окончания

Учебную практику рекомендуется проводить концентрированно.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ПРАКТИКИ

Контроль и оценка результатов освоения программы учебной практики осуществляется мастером производственного обучения в процессе проведения занятий, а также выполнения учащимися учебно-производственных заданий.

Код и наименование компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 4.1. Приемка телекоммуникационного оборудования, доставленного на монтажную площадку, с проверкой его соответствия документам ПК 4.2 Подготовка оборудования, узлов и деталей телекоммуникационного оборудования к монтажу в соответствии с проектом производства работ	«отлично» - теоретическое содержание курса освоено полностью, без пробелов, умения сформированы, все предусмотренные программой учебные задания выполнены, качество их выполнения оценено высоко; «хорошо» - теоретическое содержание курса освоено полностью, без пробелов, некоторые умения сформированы недостаточно, все предусмотренные программой учебные задания выполнены, некоторые виды заданий выполнены с ошибками; «удовлетворительно» - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые умения работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий содержат ошибки; «неудовлетворительно» - теоретическое содержание курса не освоено, необходимые умения не сформированы, выполненные учебные задания содержат грубые ошибки.	Наблюдение за ходом выполнения лабораторных работ и оценка её результатов. Оценка защиты выполнения практических заданий; оценка результатов защиты лабораторных работ и практических заданий оценка результатов защиты практических заданий; наблюдение за деятельностью обучающихся на учебной и производственной практике.