Приложение к Основной профессиональной образовательной программе

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РД
ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ТЕХНИЧЕСКИЙ КОЛЛЕДЖ ИМЕНИ Р.Н.АШУРАЛИЕВА»

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи

индекс и наименование профессионального модуля

Код и наименование специальности 11.02.15 «Инфокоммуникационные сети и системы связи»

Входящей в состав УГС 11.00.00 Электроника, радиотехника и системы связи.

Квалификация выпускника: специалист по обслуживанию телекоммуникаций

Махачкала – 2023 г.

ОДОБРЕНО

предметной (цикловой) комиссией УГС 11.00.00. Электроника, радиотехника и системы связи

Протокол № 10 от 02 июня 2023 г.

Председатель П(Ц)К

_____ _З.Н. Мирзаев_

Подпись

Рабочая программа модуля ПМ.03 «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» разработана на основе:

Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 «Инфокоммуникационные сети и системы связи» (базовой подготовки), входящей в состав укрупненной группы специальностей 11.00.00 Электроника, радиотехника и системы связи, утвержденного приказом Министерства Образования и науки Российской Федерации от 9 декабря 2016 г. № 1584, (зарегистрирован Министерством юстиции 26 декабря 2016 г., регистрационный № 44945);

с учетом:

Методических рекомендаций по разработке рабочих программ профессиональных модулей в пределах освоения основной профессиональной образовательной программы среднего профессионального образования (ППКРС и ППССЗ), разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан

в соответствии с рабочим учебным планом образовательной организации на 2023/2024 учебный год.

Разработчики:

Магомедалиева Х.Б. преподаватель дисциплин профессионального цикла ГБПОУ РД «Технический колледж имени Р.Н Ашуралиева»

Багаутдинова З.М., преподаватель дисциплин профессионального цикла ГБПОУ РД «Технический колледж им.Р.Н.Ашуралиева»

СОДЕРЖАНИЕ

стр.

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.

1.1. Область применения программы

Рабочая программа профессионального модуля – является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности (специальностям) СПО / профессии (профессиям) НПО 11.02.15 «Инфокоммуникационные сети и системы связи» в части освоения основного вида профессиональной деятельности (ВПД):

Выявления каналов утечки, установки и настройки специализированного оборудования по защите информации, проверки защищенности автоматизированных систем и информационно-коммуникационных сетей. Рабочая программа профессионального модуля может быть использована в программе профессиональной подготовки монтажника оборудования радио и телефонной связи, монтажника связи, электромонтера оборудования электросвязи и проводного вещания, электромонтера по ремонту линейно-кабельных сооружений телефонной связи и проводного вещания.

1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся в ходе освоения профессионального модуля должен:

иметь практический опыт:

- анализировать сетевую инфраструктуру;
- выявлять угрозы и уязвимости в сетевой инфраструктуре;
- разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;
- осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи
- использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.

уметь:

- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
- проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;
- определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
- осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты;

- выполнять тестирование систем с целью определения уровня защищенности;
- определять оптимальные способы обеспечения информационной безопасности;
- проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;
- проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;
- разрабатывать политику безопасности сетевых элементов и логических сетей;
- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;
- производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;
- конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
- защищать базы данных при помощи специализированных программных продуктов;
- защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.

Знать

- принципы построения информационно-коммуникационных сетей;

международные стандарты информационной безопасности для проводных и беспроводных сетей;
- нормативно - правовые и законодательные акты в области информационной безопасности;
- акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
- технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
- способы и методы обнаружения средств съёма информации в радиоканале;
- классификацию угроз сетевой безопасности;
- характерные особенности сетевых атак;
- возможные способы несанкционированного доступа к системам связи;
- правила проведения возможных проверок согласно нормативных документов ФСТЭК;
- этапы определения конфиденциальности документов объекта защиты;

назначение, классификацию и принципы работы специализированного оборудования;
- методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP.

WPA и WPA 2;
- методы и средства защиты информации в телекоммуникациях от вредоносных программ;

- технологии применения программных продуктов;
- возможные способы, места установки и настройки программных продуктов
методы и способы защиты информации, передаваемой по кабельным направляющим системам;
конфигурации защищаемых сетей;
- алгоритмы работы тестовых программ;
- средства защиты различных операционных систем и среды передачи информации;
- способы и методы шифрования (кодирование и декодирование) информации.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:
всего – 519 часов, в том числе:
максимальной учебной нагрузки обучающегося – 519 часов,
включая: обязательной аудиторной учебной нагрузки обучающегося – 296 часов; самостоятельной работы обучающегося – 37 часов,
учебной практики – 108 часов, производственной практики 72 часа, промежуточный экзамен 6 часов консультация 2ч.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности, **Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК.3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи.
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 1.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 2.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 4.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей.
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном

	и иностранном языке.

3. СТРУРКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Тематический план профессионального модуля *(вариант для НПО)*

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.							Самостоятельная работа[1]	Консультация	Экзамен
			Обучение по МДК					*Практики*				
			Всего	*В том числе*				Учебная	Производственная			
				урок	лекция	Лабораторных занятий	Практических занятий					
ПК 3.1, 3.3 ОК 01-10	Раздел 1. Программно-аппаратные средств защиты информации	169	148	70	0	28	42	-	-	21	2	6
ПК 3.1-3.3 ОК 01-10	Раздел 2. Комплексная системы защиты информации	164	148	70	0	28	42	-	-	16	2	6
ПК 3.1-3.3 ОК 01-10	Учебная практика *(по профилю специальности), часов (концентрированно)*	108						108	-			
ПК 3.1-3.3 ОК 01-10	Производственная практика *(по профилю специальности), часов (Концентрированная) практика)*	**72**							72			
	Промежуточная аттестация (экзамен)	**6**										
	Всего:	**519**	**296**	**140**	**0**	**56**	**84**	**108**	**72**	**37**	**4**	**12**

[1] Самостоятельная работа 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 профессионального модуля.

2.2. Тематический план и содержание обучения по профессиональному модулю (ПМ03)

Наименование разделов профессионального модуля (ПМ), междисциплинарных курсов (МДК) и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем часов	Коды компетенций, умений и знаний, формированию которых способствует элемент программы
1	**2**		**3**	**4**
Раздел 1. Программно-аппаратных средств защиты информации				
МДК 03.01. Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи.			**148**	
Тема 1.1. Основные понятия и анализ угроз информационной безопасности сетей. Стандарты информационной безопасности.	**Содержание учебного материала**		26	ПК 3.1, 3.3 ОК 01-10
	1.	Основные понятия защиты информации и информационной безопасности. Анализ угроз информационной безопасности.	2	
	2.	Введение в сетевой информационный обмен. Использование сети Интернет Проблемы безопасности IP-сетей	2	
	3.	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами.	2	
	4	Основные причины обострения проблемы обеспечения безопасности информационных технологий	2	
	5	Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность.	2	
	6	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.	2	
	7	Классификация угроз безопасности.	2	
	8	Принципы обеспечения безопасности информационных технологий.	2	
	9	Достоинства и недостатки различных видов мер защиты.	2	
	10	Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.	2	

	11	Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры.	2	
	12	Международные стандарты информационной безопасности Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации	2	
	13	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты.	2	
	Лабораторные работы		2	ПК 3.1, 3.3 ОК 01-10
	1.	Модель ISO/OSI и стек протоколов TCP/IP	2	
	Практические занятия.		14	ПК 3.1, 3.3 ОК 01-10
	1.	Достоинства и недостатки различных видов мер защиты.	2	
	2	Виды мер противодействия угрозам безопасности.	2	
	3	Принципы построения системы обеспечения безопасности информации	2	
	4	Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности.	2	
	5	Защита от атак по локальным и глобальным сетям	2	
	6	Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	2	
	7	Изучение способов защиты информации	2	
	Самостоятельная работа		8	ПК 3.1, 3.3 ОК 01-10
	1	Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере;	2	
	2	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	2	
	3	Ознакомление с нормативными документами по ИБ;	2	
	4	Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности;	2	

Тема 1.2. Средства защиты информации от несанкционированного доступа	**Содержание учебного материала**		12	ПК 3.1, 3.3 ОК 01-10
	1.	Основные понятия криптографической защиты информации	2	
	2	Классификация криптографических алгоритмов	2	
	3	Симметричные криптосистемы шифрования.	2	
	4	Асимметричные криптосистемы шифрования	2	
	5	Комбинированная криптосистема шифрования	2	
	6	Электронная цифровая подпись. Управление крипто ключами.	2	
	Лабораторные работы		6	
	1.	Защита компьютерной информации на уроне доступа в систему	2	ПК 3.1, 3.3ОК 01-10
	2	Защита от атак по локальным и глобальным сетям	2	
	3	Биометрическая аутентификация пользователя	2	
	Практические занятия		6	ПК 3.1, 3.3 ОК 01-10
	1.	Функция хэширования.	2	
	2	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	2	
	3	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	2	
	Самостоятельная работа		6	ПК 3.1, 3.3 ОК 01-10
	1	Составление доклада по перспективным направлениям развития средств комплексной защиты информации;	2	

	2	Разработка пакета документации по инженерно-технической защите информации на объекте;	2	
	3	Изучение возможностей инженерно-технических средств защиты информации;	2	
Тема 1.3 Обеспечение безопасности компьютерных систем и сетей	**Содержание учебного материала**		24	ПК 3.1, 3.3 ОК 01-10
	1	Технология аутентификации обеспечение безопасности операционных систем. Основные понятия аутентификации и идентификации.Аутентификация, авторизация и администрирование действий пользователей	2	
	2	Проблемы обеспечения безопасности в компьютерных системах и сетях.	2	
	3	Типовая корпоративная сеть.	2	
	4	Уязвимости и их классификация.	2	
	5	Назначение, возможности и защитные механизмы межсетевых экранов.	2	
	6	Угрозы, связанные с периметром сети.	2	
	7	Типы межсетевых экранов. Сертификация межсетевых экранов.	2	
	8	Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Виртуальные частные сети VPN на основе криптошлюза.	2	
	9	Методы аутентификации, использующие пароли и PIN-коды	2	
	10	Строгая аутентификация, основанная на симметричных и асимметричных алгоритмах. Проблемы обеспечения безопасности ОС Угрозы безопасности ОС. Понятие защищенной ОС Архитектура подсистемы защиты ОС. Функции межсетевых экранов Фильтрация трафика	2	
	11	Прикладной шлюз. Варианты исполнения МЭ. Формирование политики межсетевого взаимодействия	2	
	12	Основные понятия и функции сети VPN. Персональные и распределенные сетевые экраны.. VPN-решения для построения защищенных сетей	2	
	Лабораторные работы		10	
	1.	Аутентификация на основе PIN-кода	2	ПК 3.1, 3.3 ОК 01-10
	2	Аутентификация на основе одноразовых и многоразовых паролей	2	

	3	Основные варианты архитектуры VPN	2	
	4.	Типовая корпоративная сеть	2	
	5.	Виртуальная частная сеть VPN на основе криптошлюза	2	
	Практические занятия		12	ПК 3.1, 3.3 ОК 01-10
	1.	Исследование электронной цифровой подписи информации с использованием PGP.	2	
	2	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	2	
	3	Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа.	2	
	4	Средства обеспечения безопасности VPN	2	
	5	Особенности функционирования МЭ на различных уровнях модели OSI	2	
	6	Особенности функционирования МЭ на различных уровнях модели OSI	2	
	Самостоятельная работа		4	ПК 3.1, 3.3 ОК 01-10
	1	Изучение технических характеристик инженерно-технических средств защиты информации;	2	
	2	Разработка предложений по инженерно-технической защите информации на определенном объекте;	2	
Тема 1.4. Технологии обнаружения атак. Управление сетевой безопасностью программно-аппаратными средствами.	**Содержание учебного материала**		10	ПК 3.1, 3.3 ОК 01-10
	1.	Анализ защищенности и обнаружение атак. Средства анализа защищенности сетевых протоколов, сервисов и ОС. Методы анализа сетевой информации. Классификация систем обнаружения атак IDS. Компоненты и архитектура IDS. Методы реагирования	2	
	2.	Компьютерные вирусы и проблемы антивирусной защиты. Классификация компьютерных вирусов. Жизненный цикл вирусов.	2	
	3	Основные каналы распространения вирусов и других вредоносных программ	2	
	4	Антивирусные программы и комплексы. Построение системы антивирусной зашиты корпоративной сети.	2	
	5	Концепция глобального управления безопасностью. Функционирование системы управления программными средствами безопасности. Функционирование системы управления аппаратными средствами безопасности.	2	

	Лабораторные работы		10	ПК 3.1, 3.3 ОК 01-10
	1.	Установление и настраивание антивирусной программы DoctorWeb.	2	
	2	Установление и настраивание безопасности с помощью маршрутизатора ASUS	2	
	3	Установление и настраивание безопасности с помощью маршрутизатора TP-Link	2	
	4	Установление и настраивание безопасности с помощью маршрутизатора D- Link	2	
	5	Установление и настраивание безопасности с помощью маршрутизатора Mikro-Tik	2	
	Практические занятия		10	ПК 3.1, 3.3 ОК 01-10
	1.	МЭ Классификация сетей VPN	2	
	2	МЭ Классификация сетей VPN	2	
	3	Архитектура управления средствами сетевой безопасности.	2	
	4	Аудит и мониторинг безопасности	2	
	5	Глобальная и локальная политики безопасности	2	
	Самостоятельная работа		3	ПК 3.1, 3.3 ОК 01-10
	1	Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.	3	
Консультация 2ч экзамен 6ч				
Раздел 2. Комплексные системы защиты информации				
МДК03.02. Технология применения комплексной системы защиты информации в телекоммуникационных системах и сетях связи.			**148**	ПК 3.1, 3.3 ОК 01-10
Тема 2.1. Основы информационной безопасности	**Содержание учебного материала**		10	
	1.	Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности.	2	

	2.	Основные составляющие национальных интересов Российской Федерации в информационной сфере.	2	
	3.	Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	2	
	4	Доктрина информационной безопасности Российской Федерации.	2	
	5.	Государственная система обеспечения информационной безопасности Российской Федерации.	2	
	Практические занятия		6	ПК 3.1, 3.3 ОК 01-10
	1.	Состояние информационной безопасности РФ	2	
	2.	Общая характеристика методов и средств защиты информации.	2	
	3.	Три основные группы средств технической защиты информации	2	
	Лабораторные занятия		4	ПК 3.1, 3.3ОК 01-10
	1.	Исследование возможностей имитатора источника радиосигналов с различными видами модуляции АВРОРА-3	2	
	2.	Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга КРОНА-ПРО	2	
	Самостоятельная работа			ПК 3.1, 3.3ОК 01-10
	1	изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере;	3	
Тема 2.2 Организационно-правовые аспекты защиты информации	**Содержание учебного материала**		8	ПК 3.1, 3.3 ОК 01-10
	1.	Структура правовой защиты информации. Система документов в области защиты информации..	2	
	2	Организационные основы защиты информации. Принципы организационной защиты информации	2	
	3	Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Регулирующие организации в области защиты информации.	2	
	4	Классификация информации по категориям доступа. Критерии оценки информации. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность.	2	
	Практические занятия		8	ПК 3.1, 3.3 ОК 01-10

	1.	Обзор стандартов и методических документов в области защиты информации	2	
	2.	Категории нарушений по степени важности.	2	
	3.	Виды ответственности за правонарушения в информационной сфере	2	
	4.	Руководящие документы, регламентирующие ответственность	2	
	Лабораторные занятия		4	ПК 3.1, 3.3 ОК 01-10
	1.	Исследование принципов работы индикаторов поля РИЧ-8 / MFP-8000, ST-107, ST-165	2	
	2.	Исследование возможностей работы фильтров сетевых помехоподавляющих ЛФС-10-1Ф и ФСП-1Ф-10А	2	
	Самостоятельная работа			ПК 3.1, 3.3ОК 01-10
	1.	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации. Ознакомление с нормативными документами по ИБ.	3	
Тема 2.3. Комплексная система защиты информации	**Содержание учебного материала**		14	ПК 3.1, 3.3ОК 01-10
	1.	Общая характеристика комплексной защиты информации.	2	
	2.	Основы обеспечения комплексной защиты информации	2	
	3.	. Сущность и задачи комплексной защиты информации.	2	
	4.	Стратегии комплексной защиты информации.	2	
	5.	Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	2	
	6.	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	2	
	7.	Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	2	
	Практические занятия		6	ПК 3.1, 3.3 ОК 01-10
	1.	Структура и основные характеристики комплексной защиты информации.	2	

	2.	Способы и средства обнаружения угроз.	2	
	3.	Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.	2	
	Лабораторные занятия		6	ПК 3.1, 3.3ОК 01-10
	1.	Исследование работы генератора шума для защиты от ПЭМИН ЛГШ-501	2	
	2.	Исследование возможностей устройства для защиты объектов информатизации СОНАТА-Р2	2	
	3	Исследование возможностей устройства для защиты объектов информатизации САЛЮТ 2000Б.	2	
	Самостоятельная работа		2	ПК 3.1, 3.3ОК 01-10
	1.	Разработка пакета документации по инженерно-технической защите информации на объекте.	2	
Тема 2.4. Определение компонентов КСЗИ	**Содержание учебного материала**		14	ПК 3.1, 3.3 ОК 01-10
	1	Основы инженерно-технической защиты информации. Механические системы защиты.	2	
	2	Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации.	2	
	3	Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации.	2	
	4	Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	2	
	5	Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	2	
	6	Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания.	2	
	7	Демаскирующие признаки закладных устройств.	2	
	Практические занятия		10	ПК 3.1, 3.3 ОК 01-10
	1.	Подразделения технической защиты информации и их основные задачи.	2	
	2.	Виды НСД к информации.	2	
	3.	Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	2	

	4.	Классификация средств обнаружения и локализации закладных устройств и их излучений.	2	
	5	Классификация средств обнаружения неизлучающих закладок.	2	
	Лабораторные занятия		6	ПК 3.1, 3.3ОК 01-10
	1.	Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств ПРОКРУСТ-2000	2	
	2.	Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН СИГУРД-М19.	2	
	3.	Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля ST-165	2	
	Самостоятельная работа		2	ПК 3.1, 3.3ОК 01-10
	1.	Изучение возможностей инженерно-технических средств защиты информации.	2	
Тема 2.5. Криптографическая защита информации	**Содержание учебного материала**		12	ПК 3.1, 3.3ОК 01-10
	1.	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	2	
	2.	Симметричные криптосистемы.	2	
	3.	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	2	
	4.	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись.	2	
	5.	Технология работы электронной подписи Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC	2	
	6.	Цифровые сертификаты. Отечественный стандарт цифровой подписи	2	
	Практические занятия		12	ПК 3.1, 3.3ОК 01-10
	1.	Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	2	
	2.	Алгоритм обмена ключами Диффи-Хеллмана.	2	
	3.	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом	2	

	4.	Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом..	2	
	5.	Технология работы электронной подписи.	2	
	6.	Безопасные хеш-функции, алгоритмы хеширования.	2	
	Лабораторные занятия		4	ПК 3.1, 3.3 ОК 01-10
	1.	Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений ШЕПОТ	2	
	2.	Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов с помощью устройства КЕДР-1М	2	
	Самостоятельная работа			ПК 3.1, 3.3ОК 01-10
	1.	Изучение технических характеристик инженерно-технических средств защиты информации. - разработка предложений по инженерно-технической защите информации на определенном объекте;	3	
Тема 2. 6 Аттестация и лицензирование объектов защиты	**Содержание учебного материала**		12	ПК 3.1, 3.3ОК 01-10
	1	Общие вопросы по аттестации ОИ по требованиям безопасности информации	2	
	2	Основные стадии создания системы защиты информации на ОИ.	2	
	3	Порядок проведения аттестации объектов информатизации.	2	
	4	Организационная структура системы аттестации объектов информатизации	2	
	5	Программа и методика проведения аттестационных испытаний.	2	
	6	Лицензирование деятельности в области защиты конфиденциальной информации.	2	
	Практические занятия			ПК 3.1, 3.3ОК 01-10
	1.			
	Лабораторные занятия		4	
	1.	Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора с помощью NR-900EMS	2	ПК 3.1, 3.3ОК 01-10

	2.	Перехват компьютерной информации, несанкционированное внедрение в базы данных	2	
	Самостоятельная работа		3	ПК 3.1, 3.3ОК 01-10
	1	Разработка предложений по инженерно-технической защите информации на определенном объекте.	3	
Самостоятельная работа по ПМ 03			37	
Учебная практика (по профилю специальности) по ПМ 03 **Виды работ:** - установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов; - установка и настройка типовых программно-аппаратных средств защиты информации; - использование программно-аппаратных и инженерно-технических средств. - настройка, регулировка и ремонт оборудования средств защиты; - выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой; - проведение типовых операции настройки средств защиты операционных систем; - проведение аттестации объектов защиты; - определение источников несанкционированного доступа, исходя из модели угроз; - определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта; - обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств; - защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК; - защита информации организационными методами в соответствии с инструкциями на объекте.			108	
Производственная практика (по профилю специальности) по ПМ **Виды работ:** 1. Участие в создании комплексной системы защиты на предприятии. 2. Комплексный аудит информационной безопасности. 3. Основные задачи комплексного аудита информационной безопасности 4. Требования международных стандартов и нормативных документов в сфере информационной безопасности. 5. Поиск уязвимостей, позволяющих произвести атаку на информационную систему организации. 6. Ознакомление с основными организационно-техническими мероприятиями по защите информации 7. Применение программно-аппаратных средств защиты информации на предприятии 8. Применение инженерно-технических средств защиты информации на предприятии. 9. Применение криптографических средств защиты информации на предприятии.			72	
Промежуточная аттестация (экзамен)			6	
Всего			519	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

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

Реализация программы модуля предполагает наличие лабораторий информационной безопасности телекоммуникационной системы и информационно-коммуникационных сетей связи, полигона вычислительной техники.

Оборудование лабораторий и рабочих мест лабораторий:
- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть, проектор, экран, плазменная панель, комплект учебно-методической документации.

Оборудование полигона вычислительной техники:
- компьютеры (рабочие станции), сервер, локальная сеть, выход в глобальную сеть.

Реализация программы модуля предполагает обязательную учебную практику, которую рекомендуется проводить рассредоточено.

Оборудование и технологическое оснащение рабочих мест:
- компьютеры (рабочие станции), локальная сеть, выход в глобальную сеть.

3.2. Информационное обеспечение обучения
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

Мельников, В.П. Информационная безопасность [Текст] : учебное пособие для студентов образовательных учреждений среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 7-е изд., стер. - Москва : Академия, 2013. - 331,с. : ил., табл.; - (Среднее профессиональное образование. Информатика и вычислительная техника).; ISBN 978-5-7695-9954-5

Дополнительные источники:

1. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.: Книжный мир, 2009. — 352 с. — ISBN 978-5-8041-0378-2.
2. Петренко С. А., Курбатов В. А. Политики информационной безопасности. — М.: Компания АйТи, 2006. — 400 с. — ISBN 5-98453-024-4.
3. Петренко С. А. Управление информационными рисками. М.: Компания АйТи; ДМК Пресс, 2004. — 384 с. — ISBN 5-98453-001-5.
4. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. М.: 2000. — 428 с. — ISBN 5-93598-030-4.
5. Бармен Скотт. Разработка правил информационной безопасности. М.: Вильямс, 2002. — 208 с. — ISBN 5-8459-0323-8, ISBN 1-5787-0264-X.
6. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
7. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005).
8. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.

9. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
10. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 — 2006).
11. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
12. Словарь терминов по безопасности и криптографии. Европейский институт стандартов по электросвязи
13. Поиск. Глоссарий.ru
14. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005).
15. Государственный стандарт РФ «Аспекты безопасности. Правила включения в стандарты» (ГОСТ Р 51898-2002).
16. Домарев В. В. Безопасность информационных технологий. Системный подход — К.: ООО ТИД Диа Софт, 2004. — 992 с.
17. Зайцев А. П. Технические средства и методы защиты информации: Учебник для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В.Мещеряков; Под ред. А.П.Зайцева - 7 изд., исправ. - М.: Гор. линия-Телеком, 2012. - 442с.; 60x90 1/16 - (Уч. для вузов). (о) ISBN 978-5-9912-0233-6 (znanium.com)
18. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2Партыка Т. Л. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов И. И., 5-е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-627-0, 200 экз.(znanium.com)
19. Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с.: 60x90 1/16. - (Высшее образование: Бакалавриат; Магистратура). (переплет) ISBN 978-5-369-01378-6, 500 экз. (znanium.com)

Научно-технические и реферативные журналы:

1. Электросвязь
2. Вестник связи
3. Сети и системы связи
4. Мобильные системы
5. Цифровая обработка сигналов
6. Сводный реферативный журнал "Связь".

Печатные издания

1. Партыка Т.Л. Вычислительная техника : учеб. пособие / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — М. : ФОРУМ : ИНФРА-М, 2017. — 445 с. : ил. — (Среднее профессиональное образование). ISBN: 978-5-91134-646-1

2.. Арутюнов, В. В. Защита информации : учебно-методическое пособие / В. В. Арутюнов. - Москва : Либерея-Бибинформ, 2008. - 55, с. : рис. ; 21 см. - (Библиотекарь и время. XXI век ; № 99). - ISBN 5-85129-175-3

3. Васильков А. В., Васильков А. А., Васильков И. А. Информационные системы и их безопасность: Учебное пособие. - М.: Форум, 2015. - 528 с.: 60x90 1/16. - (Профессиональное образование) (Переплёт) ISBN 978-5-91134-289-0

4. Мельников, В.П. Информационная безопасность: учебное пособие для студентов образовательных учреждений среднего профессионального образования / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 7-е изд., стер. - Москва : Академия,

2013. - 331, [1] с. : ил., табл.; - (Среднее профессиональное образование. Информатика и вычислительная техника).; ISBN 978-5-7695-9954-5
5.Эксплуатация объектов сетевой инфраструктуры: учебник/А.В.Назаров.- М.: Академия, 2014.- 368с. ISBN 978-5-44680347-7

Интернет ресурсы:
Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, WWW.twirpx.com, WWW.referent.ru, WWW.kodeks-luks.ru/dws, WWW.Consultant.ru/online.

3.3. Общие требования к организации образовательного процесса

Обязательным условием допуска к учебной практике в рамках профессионального модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи» является освоение учебной практики для получения первичных профессиональных навыков в рамках профессионального модуля «Разработка программных модулей программного обеспечения для компьютерных систем».

Перед изучением модуля обучающиеся изучают следующие дисциплины «Компьютерное моделирование», «Теория электрических цепей», «Технология монтажа телекоммуникационных систем и информационно-коммуникационных сетей связи», «Основы программирования», «Правовое обеспечение профессиональной деятельности», «Безопасность жизнедеятельности».

3.4. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарному курсу (курсам)**:** наличие высшего профессионального образования, соответствующего профилю модуля «Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи».
Требования к квалификации педагогических кадров, осуществляющих руководство практикой
Инженерно-педагогический состав: высшее инженерное образование, соответствующее профилю модуля.
Мастера: обязательная стажировка в профильных организациях не реже 1-го раза в 3 года. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК.2.1. Использовать программно-аппаратные средства защиты информации в телекоммуникационных системах и сетях связи.	- Установление и настройка специализированного оборудования по защите информации;	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования;- контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля.
	- Установление и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей связи; - Выявление возможных атак на автоматизированные системы;	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
	- Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей	
	- Организация защиты в различных операционных системах и средах, шифрования информации.	
ПК.2.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению	- Классифицировать угрозы информационной безопасности;	- Текущий контроль в форме:- защиты лабораторных занятий;- тестирования; - - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля.
	- проводить выборку средств защиты в соответствии с выявленными угрозами; определять возможные виды атак; - осуществлять мероприятия по проведению аттестационных работ; - разрабатывать политику безопасности объекта; выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;	- Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования. - Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике

		и по разделу профессионального модуля.
	- использовать программные продукты, выявляющие недостатки систем защиты;	- Текущий контроль в форме:- защиты лабораторных занятий; - - тестирования; - - контрольных работ по темам МДК. - Экзамены по разделу профессионального модуля.
	- производить установку и настройку средств защиты; конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;	- Текущий контроль в форме:- защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
	- выполнять тестирование систем с целью определения уровня защищенности; - использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации;	- Текущий контроль в форме: - - защиты лабораторных занятий; - Зачеты по учебной практике и по разделу профессионального модуля.
ПК 2.3. Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.	- классификацию и принципы работы специализированного оборудования;	Текущий контроль в форме:- защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК. Экзамены по разделу профессионального модуля.
	- принципы построения информационно-коммуникационных сетей;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования.
	- возможные способы несанкционированного доступа; нормативно-правовые и законодательные акты в области информационной безопасности;	Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля.

	- правила проведения возможных проверок; этапы определения конфиденциальности документов объекта защиты; - технологии применения программных продуктов; возможные способы, места установки и настройки программных продуктов; - конфигурации защищаемых сетей; алгоритмы работы тестовых программ; собственные средства защиты различных операционных систем и сред; - способы и методы шифрования информации выявления каналов утечки информации; определения необходимых средств защиты;	Текущий контроль в форме: - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК. Экзамены по разделу профессионального модуля. Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля. Текущий контроль в форме: - защиты лабораторных занятий; Зачеты по учебной практике и по разделу профессионального модуля. Текущий контроль в форме: - защиты лабораторных занятий; - тестирования; - контрольных работ по темам МДК.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	– демонстрация интереса к будущей профессии	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	– выбор и применение методов и способов решения профессиональных задач в области разработки и администрирования баз данных; – оценка эффективности и качества выполнения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.	– решение стандартных и нестандартных профессиональных задач в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	– эффективный поиск необходимой информации; – использование различных источников, включая электронные	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.	– разрабатывать, программировать и администрировать базы данных	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.	– взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.	– самоанализ и коррекция результатов собственной работы	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	– организация самостоятельных занятий при изучении профессионального модуля	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы
ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.	– анализ инноваций в области разработки и администрирования баз данных	Интерпретация результатов наблюдений за деятельностью обучающегося в

		процессе освоения образовательной программы
ОК 10. Исполнять воинскую обязанность, в том числе с применением полученных профессиональных знаний (для юношей).	– решение ситуативных задач, связанных с использованием профессиональных компетенций	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы

Разработчики:

ГБПОУ РД ТК
им Р.Н Ашуралиева преподаватель дисциплин профессионального цикла Х.Б.Магомедалиева
(место работы) (занимаемая должность) (инициалы, фамилия)

ГБПОУ РД ТК
им Р.Н Ашуралиева преподаватель дисциплин профессионального цикла З.М Багаутдинова
(место работы) (занимаемая должность) (инициалы, фамилия)

Эксперты:

_____ _____ _____
(место работы) (занимаемая должность) (инициалы, фамилия)

РЕЦЕНЗИЯ
на рабочую программу
учебной дисциплины « ПМ.03 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.»

На рецензию представлена рабочая программа профессионального модуля «ПМ.03 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.», разработчиком которой является преподаватель ГБПОУ «Технический колледж имени Р.Н Ашуралиева» Магомедалиева Хадыжа-Ханум Борисовна и Багаутдинова Зарема Магомедзапировна.

Рабочая программа профессионального модуля «ПМ.03 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи.» разработана на основе требований ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи, в соответствии с рабочим учебным планом образовательной организации на 2023/2024 учебный год, с учетом Методических рекомендаций по разработке рабочей программы профессионального модуля при реализации основной профессиональной образовательной программы среднего профессионального образования (ППКРС И ППССЗ) разработанных Отделом профессионального образования Министерства образования и науки Республики Дагестан.

Профессиональный модуль ПМ.03 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. является обязательной частью модульного цикла ППССЗ.

Рабочая программы профессионального модуля включает: титульный лист, содержание, раздел 1 «Паспорт рабочей программы учебной дисциплины», раздел 2 «Структура и примерное содержание профессионального модуля», раздел 3 «Условия реализации профессионального модуля», раздел 4 «Контроль и оценка результатов освоения профессионального модуля», Все разделы программы представлены и выполнены в соответствии с рекомендованной формой.

В паспорте программы указываются область применения программы, место профессионального модуля в структуре программы подготовки специалистов среднего звена, Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля, количество часов на освоение программы профессионального модуля.

В тематическом плане программы профессионального модуля. содержится почасовое распределение видов учебной работы студентов, обеспечивается логическая последовательность и четкость в наименовании разделов и тем. Содержание теоретического материала, практических занятий и самостоятельной работы студентов соответствует целям и задачам освоения профессионального модуля, уровни освоения обозначаются дидактически целесообразно.

Перечисленное оборудование лаборатории и рабочих мест лаборатории, в том числе персональные компьютеры с необходимым комплектом лицензионного программного обеспечения, технические средства обучения, печатные и электронные издания основной и дополнительной литературы, обеспечивают материально-технические и информационные условия реализации программы профессионального модуля.

В качестве рекомендаций составителю рабочей программы профессионального модуля предлагается ежегодно корректировать содержание теоретических и практических занятий с учётом новых тенденций в области информационных технологий, обновлять перечень информационных источников.

Представленная на рецензию рабочая программа профессиональный модуль ПМ.03 Обеспечение информационной безопасности телекоммуникационных систем и информационно-коммуникационных сетей связи. рекомендуется к практическому применению в образовательном процессе в профессиональных образовательных организациях, реализующих программу подготовки специалистов среднего звена по специальности 11.02.15 Инфокоммуникационные сети и системы связи..

Рецензент _____ М.А Абдулаев генеральный директор ООО «Каспий-Телеком»