

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«ПОВОЛЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ  
УНИВЕРСИТЕТ»

**ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»**



УТВЕРЖДАЮ

Заместитель директора по УМР

 Е.Ю. Кузнецов

«28» апреля 2023 г.

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ  
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ  
СИСТЕМ РАДИОСВЯЗИ, МОБИЛЬНОЙ СВЯЗИ И  
ТЕЛЕРАДИОВЕЩАНИЯ**

по специальности 11.02.18 Системы радиосвязи, мобильной связи и  
телерадиовещания

## РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 7

«27» апреля 2023 г.

Председатель ПЦК  /Е.Ю. Кузнецов/

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания разработана на основе федерального государственного образовательного стандарта среднего профессионального образования по специальности Системы радиосвязи, мобильной связи и телерадиовещания, утвержденного Приказом Минпросвещения России от 11.11.2022 № 963.

Разработчик:

Смирнов Владимир Иванович, старший преподаватель кафедры информационной безопасности ФГБОУ ВО «ПГТУ».

Рецензент (внутренний)

Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа «Политехник».

Рецензент (внешний)

Еросланов С.Г., директор сервисного центра г. Йошкар-Ола филиала Республики Марий Эл ПАО «Ростелеком».

## **СОДЕРЖАНИЕ**

1. АННОТАЦИЯ
2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ  
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

## 1. АННОТАЦИЯ

Профессиональный модуль ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания относится к профессиональному циклу по программе подготовки специалистов среднего звена, устанавливающей базовые знания по специальности среднего профессионального образования 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

Общий объем учебной нагрузки по профессиональному модулю составляет 339 часов, нагрузка во взаимодействии с преподавателем составляет 144 часа, часов самостоятельной работы – 13.

Содержание профессионального модуля включает изучение разделов междисциплинарных курсов:

Раздел 1. Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания.

Текущий контроль проводится в форме оценки тестирования, экспертного наблюдения за выполнением практических работ, оценки процесса и результатов выполнения видов работ на практике.

Форма промежуточной аттестации – экзамен, экзамен (квалификационный).

## **2. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

### **2.1. Место профессионального модуля в структуре программы подготовки специалистов среднего звена.**

Профессиональный модуль ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания.

### **2.2. Цель и планируемые результаты освоения профессионального модуля**

В результате освоения профессионального модуля ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания обучающийся должен обладать предусмотренными ФГОС СПО по специальности 11.02.18 Системы радиосвязи, мобильной связи и телерадиовещания умениями, знаниями, которые формируют следующие **профессиональные компетенции**.

<b>Код</b>	<b>Наименование результата обучения</b>
ПК 3.1	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности.
ПК 3.2	Разрабатывать комплекс методов и средств защиты информации в системах радиосвязи, мобильной связи и телерадиовещания.
ПК 3.3	Осуществлять текущее администрирование для защиты систем радиосвязи, мобильной связи и телерадиовещания с использованием специализированного программного обеспечения и оборудования.

Освоение профессионального модуля направлено на развитие **общих компетенций**.

<b>Код Результата обучения</b>	<b>Результат обучения</b>
<b>1</b>	<b>2</b>
<b>Общие компетенции</b>	
ОК 01	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам.
ОК 02	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях.
ОК 04	Эффективно взаимодействовать и работать в коллективе и команде.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста.

ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, 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	Пользоваться профессиональной документацией на государственном и иностранном языках.

### Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся должен:

иметь практически й опыт	<ul style="list-style-type: none"> <li>- анализе сетевой инфраструктуры;</li> <li>- выявлении угроз и уязвимости в сетевой инфраструктуре;</li> <li>- разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;</li> <li>- осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;</li> <li>- использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.</li> </ul>
уметь	<ul style="list-style-type: none"> <li>- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;</li> <li>- определять оптимальные способы обеспечения информационной безопасности;</li> <li>- осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;</li> <li>- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов</li> <li>- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;</li> <li>- защищать базы данных при помощи специализированных программных продуктов.</li> </ul>
знать	<ul style="list-style-type: none"> <li>- принципы построения систем радиосвязи, мобильной связи и телерадиовещания;</li> <li>- международные стандарты информационной безопасности;</li> <li>- акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;</li> <li>- технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;</li> <li>- классификацию угроз сетевой безопасности;</li> <li>- методы и способы защиты информации, передаваемой по кабельным направляющим системам;</li> <li>- правила проведения возможных проверок согласно нормативным документам ФСТЭК;</li> <li>- средства защиты различных операционных систем и среды передачи информации.</li> </ul>

### **2.3. Количество часов, отводимое на освоение профессионального модуля:**

Всего часов – 339 часов, в том числе:

на освоение МДК - 177 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося– 144 часа;

самостоятельной работы обучающегося– 13 часов;

на практики: учебную – 72 часа, производственную –72 часа.

### 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

#### 3.1. Структура профессионального модуля

#### ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания

Код профессиональных и общих компетенций	Наименования разделов профессионального модуля	Всего часов	Объем времени, отведенный на освоение междисциплинарного курса (курсов)								Практика	
			Обязательная аудиторная учебная нагрузка обучающегося					Самостоятельная работа обучающегося, часов	консультации часов	Промежуточная аттестация	Учебная, часов	Производственная часов
			Всего, часов	теоретическое	практические занятия, часов	лабораторные занятия, часов	в т.ч., курсовая работа (проект), часов					
1	2	3	4	5	6	7	8	9	10	11	12	13
ПК 3.1-3.3 ОК 01-09	Раздел 1. Технология монтажа и эксплуатация средств радио- и мобильной связи.	177	144	68	-	76	-	13	2	18	72 (2 нед)	72 (2 нед)
ПК 3.1-3.3 ОК 01-09	Учебная практика	72	-	-	-	-	-	-	-	-		
	Производственная практика (по профилю специальности)	72	-	-	-	-	-	-	-	-		
	Экзамен (квалификационный)	18	-	-	-	-	-	-	-	18		
Всего:		339	144	68	-	76	-	13	2	36	72	72



### 3.2. Тематический план и содержание профессионального модуля

#### ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания

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
<b>Раздел 1. Обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания</b>		<b>177</b>
<b>МДК 03.01. Технология обеспечения информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания</b>		<b>177</b>
Тема 1.1. Основы безопасности информационных технологий.	<b>Содержание учебного материала</b>	<b>42</b>
	1. Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем. Основные причины обострения проблемы обеспечения безопасности информационных технологий.	22
	2. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.	
	3. Угрозы безопасности информационных технологий. Классификация угроз безопасности.	
	4. Принципы обеспечения безопасности информационных технологий Принципы построения системы обеспечения безопасности информации в автоматизированной системе.	
	5 Стандарты информационной безопасности систем мобильной связи. Особенности решений по информационной безопасности в беспроводных стандартах IEEE 802.11, IEEE 802.16, DECT и системах сотовой связи GSM, CDMA.	
	<b>Лабораторные занятия</b>	16
	1 Анализ современных угроз ИБ.	
	2 -3 Проектирование границ защиты.	
	4-5 Применение сертификатов для аутентификации и авторизации.	
	6-7 Исследование и разработка политики информационной безопасности объекта (предприятия).	
	8 Сравнительное исследование информационной безопасности систем мобильной связи.	
	<b>Самостоятельная работа обучающегося</b>	4
	1. Составить кроссворд на тему: «Основные понятия информационной безопасности».	
Тема 1.2. Обеспечение	<b>Содержание учебного материала</b>	<b>50</b>

безопасности информационных технологий.	Особенности обеспечения информационной безопасности в компьютерных сетях. Спецификация средств защиты в компьютерных сетях.	22
	Сетевые модели передачи данных. Модель взаимодействия открытых систем OSI/ISO. Структура пакета. Шифрование.	
	Типовые удаленные атаки и их характеристика. Принципы защиты распределенных вычислительных сетей. Принципы построения защищенных вычислительных сетей.	
	Безопасность операционных систем. Проблемы обеспечения безопасности операционных систем, угрозы безопасности, защищенная операционная система.	
	Архитектура подсистемы защиты операционных систем. Функции подсистемы защиты операционных систем, идентификация, аутентификация и авторизация доступа в операционные системы, разграничение доступа, аудит.	
	<b>Лабораторные занятия</b>	24
	9-11 Установка СЗИ (На примере IWTM).	
	12-14 Установка межсетевого экрана (На примере Cisco NGFW).	
	15-17 Настройка правил фильтрации трафика DLP системой.	
	18-20 Настройка уровней доступа к различным подсетям.	
	<b>Самостоятельная работа обучающегося</b>	4
	1. Подготовить презентацию по теме: «Виды уязвимости информации и формы ее проявления.	
Тема 1.3. Обеспечение безопасности стандартными средствами защиты.	<b>Содержание учебного материала</b>	<b>28</b>
	Локальные политики безопасности.	12
	Пользователи, типы пользователей, создание и ограничение пользователей (windows, unix-подобные ОС).	
	Построение виртуальных защищенных сетей (VPN). Основные понятия, классификация и функции сетей VPN, средства обеспечения безопасности VPN, варианты архитектуры и принципы построения виртуальных защищенных каналов, достоинства применения технологий VPN.	
	<b>Лабораторные занятия</b>	16
	21-22 Настройка локальных политик (windows системы).	
	23 Создание пользователей, административная, пользовательская, гостевая учетные записи (windows системы).	
	24-26 Создание пользователей, права суперпользователя, ограничения пользователей, права доступа (unix системы).	

	27-28 Построение фрагмента виртуальной защищенной сети.	
Тема 1.4 Технологии межсетевых экранов.	<b>Содержание учебного материала</b>	<b>10</b>
	Функции межсетевых экранов. Фильтрация трафика, выполнение функций посредничества, дополнительные возможности межсетевых экранов.	4
	Особенности функционирования межсетевых экранов сетей связи. Прикладной шлюз, варианты исполнения межсетевых экранов, формирование политики межсетевого взаимодействия, схемы подключения межсетевых экранов, персональные и распределенные межсетевые экраны, проблемы безопасности межсетевых экранов.	
	<b>Лабораторные занятия</b>	6
	29 Установка и настройка межсетевых экранов.	
	30 Выявление возможных атак на автоматизированные системы и применение различных функций межсетевых экранов.	
	31 Конфигурирование операционной системы.	
Тема 1.5. Криптографическая защита информации.	<b>Содержание учебного материала</b>	<b>27</b>
	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	8
	Симметричные криптосистемы. Ассиметричные криптосистемы.	
	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	
	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа.	
	<b>Лабораторные занятия</b>	14
	32-33 Шифрование данных симметричными и ассиметричными алгоритмами.	5
	34-35 Криптоанализ.	
	36-37 Шифрование трафика, шифрование данных.	
	38 Исследование методов криптосистем с открытым ключом.	
	<b>Самостоятельная работа обучающегося</b>	
	1. Составление таблицы «Сравнительные характеристики методов криптографической защиты информации».	
<b>Консультация</b>		<b>2</b>

<b>Промежуточная аттестация</b>	<b>18</b>
<b>Учебная практика</b> <b>Виды работ</b> 1. Классификация угроз информационной безопасности в инфокоммуникационных системах и сетях связи с предоставлением услуг мобильной связи и телевидения. 2. Определение оптимального способа обеспечения информационной безопасности. 3. Мероприятия по проведению аттестационных работ и выявлению каналов утечки. 4. Выявление недостатков систем защиты в системах и сетях связи с использованием специализированных программных продуктов. 5. Расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей. 6. Защита баз данных при помощи специализированных программных продуктов.	72
<b>Производственная практика (если предусмотрена итоговая (концентрированная) практика)</b> <b>Виды работ</b> 1. Анализ сетевой инфраструктуры систем с предоставлением услуг мобильной связи и телевидения. 2. Угрозы и уязвимости в сетевой инфраструктуре. 3. Разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи с предоставлением услуг мобильной связи и телевидения. 4. Администрирование для защиты инфокоммуникационных сетей и систем связи с предоставлением услуг мобильной связи и телевидения. 5. Специализированное программное обеспечение и оборудование для защиты инфокоммуникационных сетей и систем связи с предоставлением услуг мобильной связи и телевидения.	72
<b>Экзамен (квалификационный)</b>	<b>18</b>
<b>Всего</b>	<b>339</b>

## **4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

### **4.1. Материально-техническое обеспечение профессионального модуля**

#### **ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания.**

Реализация профессионального модуля требует наличия лаборатории информационной безопасности телекоммуникационных систем.

##### **Оснащение лаборатории.**

##### **Комплект мебели для учебного процесса.**

**Мультимедийное оборудование:** персональные компьютеры – 22 шт., проектор мультимедийный Hitachi CP-X1250, разветвитель видеосигнала; принтер HP LaserJet Professional P1102.

**Средства обучения:** комплект наглядных пособий «Технические средства информатизации», техническая документация на технические средства информатизации, комплект презентаций; анализатор линейных коммуникаций ULAN-2; приёмник «Скорпион» поисковый, скоростной Ver 3.5; контрольное устройство ТЕСТ-031; multifunctional поисковый прибор ST 031; нелинейный лоатор SEL SP-61/М «Катран»; указатель проводки UP-7; генератор шума ГШ-2500; комплекс защиты информации в составе PCI-плата, ПО SN-5, считыватель, 2 идентификатора; комплекс защиты информации Secret Net 5.0; программно-аппаратные средства защиты информации от НСД, блокировки доступа и нарушения целостности (комплекс защиты информации Secret Net 5.0, комплекс защиты информации Secret Disc 4.0 аппаратный комплекс АККОРД - AMD3 - 5.5, аппаратный комплекс АККОРД -AMD3 - 5MX, аппаратный комплекс АККОРД -AMD3 — 5.5 E, аппаратный комплекс СЗИ НСД АККОРД –AMD, подсистема распределённого аудита и управления «Аккорд-РАУ» (2 CD + ТМ ключ DS-1996), аппаратно-программный модуль доверенной загрузки с удалённым управлением для шины PCI-Express M-526E1 (АПМДЗ-УМ1 исполнение 1, КРИПТОН-ЗАМОК/Е) – 3 шт.); система вибро-акустической защиты «Соната-АВ»; устройство защиты «Соната-PC2»; устройство защиты «Соната-Р2»; виброизлучатель ВИ-45 – 5шт.; адаптер DWA-160-10 шт; DAP-2310 – 5шт.; DES-3200-28 – 8шт.; DES-3810-28 -2шт.; коммутатор D-Link DES-1005 – 5шт.; коммутатор D-Link DIR-615 – 5 шт.; коммутатор D-Link DES-1100-16 -5 шт.; кримпер NT-2008AR; кабельный тестер NCT-1; тестер кабельный TC-NT2; SMART-Card Алладин – 2шт; ASEDrive IIIe V2C- 2 шт.; электронный ключ eToken – 8шт.; программные средства криптографической защиты информации (ПСКЗИ «Шипка 2.0» (диск + УСБ-устройство) -5шт); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (3 CD); программно-аппаратный комплекс СЗИ НСД «Аккорд-WIN64» (2 CD)- 3 шт; программно-аппаратный комплекс «Соболь» (PCI-плата,CD-диск ПО, соединитель) – 3 шт.; экран настенный 200\*200см Braun Roll Vision.

##### **Перечень лицензионного программного обеспечения:**

- Microsoft Access (лицензия №IM123460);
- Microsoft Office Standard (лицензия №66059532 OPEN 96044930ZZE1711);
- Microsoft Project Professional (лицензия №IM123460);
- Microsoft Visio Professional (лицензия №IM123460);
- Microsoft Visual Studio Enterprise (лицензия №IM123460);

- Microsoft Windows Enterprise (лицензия №IM123460);
- антивирусный программный комплекс: Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2);
- комплект ГАРАНТ–Мастер (лицензия №12–40272–000898);
- программные и программно-аппаратные средства обнаружения вторжений (Snort 2.9 (свободно распр. ПО),
- Nmap 7.8 (свободно распр. ПО);
- средства уничтожения остаточной информации в запоминающих устройствах («СГУ–2» демоверсия (свободно распр. ПО);
- комплект ПО для решения основных пользовательских задач (свободно распр. ПО); - справочная правовая система «Консультант Плюс» (контракт №2023\_CB\_3 от 29.12.2022г);
- программные средства выявления уязвимостей в АС и СБТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО),
- Metasploit Framework (свободно распр. ПО);
- программные средства криптографической защиты информации (КриптоПро CSP 5.0 (лицензионный контракт №010/IO20-002792 от 28.08.20),
- ViPNet CSP 4 (свободно-распространяемое);
- программные средства защиты среды виртуализации (VM Monitor (свободно распр. ПО), Zabbix (свободно распр. ПО).

## 4.2. Информационное обеспечение профессионального модуля

### Основная и дополнительная литература

№ п/п	Список используемой литературы (печатные издания, электронные издания за последние 5 лет)	Количество экземпляров, имеющих в библиотеке, или ссылка на ЭБС
<b>ОСНОВНАЯ ЛИТЕРАТУРА</b>		
1.	<b>Гилязова, Р.Н.</b> Информационная безопасность. Лабораторный практикум: учебное пособие для СПО / Р.Н. Гилязова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 44 с. — ISBN 978-5-8114-8249-8. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/173796">https://e.lanbook.com/book/173796</a> (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.	электронный ресурс
2.	<b>Никифоров, С.Н.</b> Методы защиты информации. Защита от внешних вторжений: учебное пособие / С.Н. Никифоров. — Санкт-Петербург: Лань, 2020. — 96 с. — ISBN 978-5-8114-5720-5. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/146802">https://e.lanbook.com/book/146802</a> (дата обращения: 27.11.2020). — Режим доступа: для авториз. пользователей.	электронный ресурс
3.	<b>Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации:</b> учебник / сост. И.Г. Дровникова, А.В. Калач, И.И. Лившиц [и др]. - Воронеж: Научная книга, 2022. - 304 с. - ISBN 978-5-4446-1743-4. - Текст: электронный. - URL: <a href="https://znanium.com/catalog/product/1999941">https://znanium.com/catalog/product/1999941</a> (дата обращения: 29.08.2023). — Режим доступа: по подписке.	электронный ресурс

	<a href="https://znanium.com/catalog/document?id=426504#bib">https://znanium.com/catalog/document?id=426504#bib</a>	
4.	<b>Хорев, П.Б.</b> Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - Москва: ФОРУМ: ИНФРА-М, 2021. - 352 с. - (Среднее профессиональное образование) - <a href="https://znanium.com/read?id=364477">https://znanium.com/read?id=364477</a>	электронный ресурс
<b>ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА</b>		
	Учебники, учебные пособия	
1.	<b>Ищейнов, В.Я.</b> Основные положения информационной безопасности: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - Москва: ФОРУМ: ИНФРА-М, 2021. - 208 с. - (Среднее профессиональное образование) - <a href="https://znanium.com/read?id=365084">https://znanium.com/read?id=365084</a>	электронный ресурс
2.	<b>Петренко, В.И.</b> Защита персональных данных в информационных системах. Практикум: учебное пособие для СПО / В.И. Петренко, И.В. Мандрица. — Санкт-Петербург: Лань, 2021. — 108 с. — ISBN 978-5-8114-6924-6. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/153678">https://e.lanbook.com/book/153678</a> (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.	электронный ресурс
3.	<b>Прохорова, О.В.</b> Информационная безопасность и защита информации: учебник для СПО / О.В. Прохорова. — 2-е изд., стер. — Санкт-Петербург: Лань, 2021. — 124 с. — ISBN 978-5-8114-7338-0. — Текст: электронный // Лань: электронно-библиотечная система. — URL: <a href="https://e.lanbook.com/book/158939">https://e.lanbook.com/book/158939</a> (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.	электронный ресурс

## **5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Контроль и оценка результатов освоения профессионального модуля осуществляется преподавателем в форме текущего контроля успеваемости и промежуточной аттестации.

Промежуточная аттестация имеет целью определить степень достижения запланированных результатов обучения по профессиональному модулю за период обучения. Форма промежуточной аттестации - экзамен, экзамен (квалификационный).

Текущий контроль успеваемости осуществляется в процессе проведения практических занятий, обеспечивает оценивание хода освоения модуля.

Формы текущего контроля успеваемости: тестирование, устный опрос, доклады, выполнение практических работ.



№	Наименование раздела	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
1.	Технология монтажа и эксплуатация средств радио- и мобильной связи.	ПК 3.1-3.3 ОК 01-09	<ul style="list-style-type: none"> <li>- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;</li> <li>- определять оптимальные способы обеспечения информационной безопасности;</li> <li>- осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;</li> <li>- выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов</li> <li>- выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;</li> <li>- защищать базы данных при помощи специализированных программных продуктов.</li> </ul>	<ul style="list-style-type: none"> <li>- принципы построения систем радиосвязи, мобильной связи и телерадиовещания;</li> <li>- международные стандарты информационной безопасности;</li> <li>- акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;</li> <li>- технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;</li> <li>- классификацию угроз сетевой безопасности;</li> <li>- методы и способы защиты информации, передаваемой по кабельным направляющим системам;</li> <li>- правила проведения возможных проверок согласно нормативным документам ФСТЭК;</li> <li>- средства защиты различных операционных систем и среды передачи информации.</li> </ul>	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практическом обучении.</p> <p>Экзамен, экзамен (квалификационный) по профессиональному модулю.</p>

## **Критерии оценивания результатов обучения по профессиональному модулю, шкала оценивания**

### Критерии оценивания:

- усвоение программного теоретического материала (объем знаний, глубина усвоения);
- умение излагать программный материал (четкость, грамотность изложения материала, точность и полнота воспроизведения учебного материала);
- умение применять теоретические знания на практике.

### Шкала оценивания:

Результаты сдачи экзамена, экзамена (квалификационного) оцениваются по шкале «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка «отлично» выставляется обучающемуся, который глубоко и прочно усвоил программный материал, проявляет знание основной и дополнительной литературы, грамотно, логически стройно и аргументировано излагает материал, дает исчерпывающие ответы на поставленные вопросы. В ответе тесно увязывается теория с практикой, при этом обучающийся не затрудняется с ответом при видоизменении задания, свободно справляется с практическими заданиями.

Оценка «хорошо» выставляется обучающемуся, твердо знающему программный материал, который излагает его грамотно и по существу, не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, не испытывает затруднений с ответами на вопросы.

Оценка «удовлетворительно» выставляется обучающемуся, который имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, испытывает затруднения при выполнении практических работ.

Оценка «неудовлетворительно» выставляется обучающемуся, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

## **Дополнения и изменения к рабочей программе на учебный год**

Дополнения и изменения к рабочей программе на 2024-2025 учебный год по профессиональному модулю ПМ.03 Обеспечение информационной безопасности систем радиосвязи, мобильной связи и телерадиовещания: в раздел Условия реализации профессионального модуля (пункт Информационное обеспечение профессионального модуля) внесены изменения в список основной и дополнительной литературы.

Дополнения и изменения в рабочей программе обсуждены на заседании ПЦК общетехнических дисциплин.

«30» августа 2024 г. (протокол № 1)

Председатель ПЦК  /Кузнецов Е.Ю./