

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

ВЫСШИЙ КОЛЛЕДЖ «ПОЛИТЕХНИК»



УТВЕРЖДАЮ

Заместитель директора по УМР

Е. Ю. Кузнецов

«29» апреля 2022 г.

**РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ ВЕЩАНИЯ**

по специальности 11.02.10 Радиосвязь, радиовещание и телевидение

РАССМОТРЕНА И ОДОБРЕНА

Предметно-цикловой комиссией

Протокол № 5

«28» апреля 2022 г.

Председатель ПЦК  /Е.Ю. Кузнецов/

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания разработана на основе Федерального государственного образовательного стандарта по специальности 11.02.10 Радиосвязь, радиовещание и телевидение.

Организация-разработчик: Высший колледж ПГТУ «Политехник».

Разработчик:

Савинов Александр Николаевич, к.т.н., доцент кафедры ФГБОУ ВО «ПГТУ».

Рецензент (внутренний)

Кузнецов Е.Ю., к.т.н., заместитель директора по УМР Высшего колледжа ПГТУ «Политехник».

Рецензент (внешний)

Баев А.А., канд. техн. наук, зав. каф радиотехнических и медико-биологических систем ФГБОУ ВО «ПГТУ».

Рецензент (представитель работодателя)

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 в телекоммуникационных системах и сетях вещания относится к профессиональному циклу по программе подготовки специалистов среднего звена, устанавливающей базовые знания по специальности среднего профессионального образования 11.02.10 Радиосвязь, радиовещание и телевидение.

Общий объем учебной нагрузки по профессиональному модулю составляет 382 часа, нагрузка во взаимодействии с преподавателем составляет 208 часов, часов самостоятельной работы – 102.

Содержание профессионального модуля включает изучение разделов междисциплинарных курсов:

МДК 03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и радиовещания:

1. Основы информационной безопасности.
2. Правовое обеспечение информационной безопасности.
3. Организационное обеспечение информационной безопасности.

МДК 03.02 Технология использования систем условного доступа в сетях вещания:

1. Программно-аппаратные средства защиты информации.
2. Администрирование телекоммуникационных систем и сетей связи.

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 – дифференцированный зачет, 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 в телекоммуникационных системах и сетях вещания относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования 11.02.10 Радиосвязь, радиовещание и телевидение.

2.2. Цель и планируемые результаты освоения профессионального модуля.

В результате освоения профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания обучающийся должен обладать предусмотренными ФГОС СПО по специальности 11.02.10 Радиосвязь, радиовещание и телевидение умениями, знаниями, которые формируют следующие **профессиональные компетенции**:

Код	Наименование результата обучения
ПК 3.1	Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.
ПК 3.2	Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.
ПК 3.3	Обеспечивать безопасное администрирование сетей вещания.

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

Код	Наименование результата обучения
ОК 1	Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.
ОК 2	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.
ОК 3	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.
ОК 4	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.
ОК 5	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.
ОК 8	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.
ОК 9	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся должен:

иметь практический и опыт	<ul style="list-style-type: none"> – выявления каналов утечки информации; – определения необходимых средств защиты; – проведения аттестации объекта защиты (проверки уровня защищенности); – разработки политики безопасности для объекта защиты; – установки, настройки специализированного оборудования по защите информации; – выявления возможных атак на автоматизированные системы; – установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей; – конфигурирования автоматизированных систем и информационно-коммуникационных сетей; – проверки защищенности автоматизированных систем и информационно-коммуникационных сетей; – защиты баз данных; – организации защиты в различных операционных системах и средах; – шифрования информации
уметь	<ul style="list-style-type: none"> – классифицировать угрозы информационной безопасности; – 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; – использовать программные продукты, выявляющие недостатки систем защиты; – производить установку и настройку средств защиты; – конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; – выполнять тестирование систем с целью определения уровня защищенности; – использовать программные продукты для защиты баз данных; – применять криптографические методы защиты информации
знать	<ul style="list-style-type: none"> – каналы утечки информации; – назначение, классификацию и принципы работы специализированного оборудования; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; – законодательные и нормативные правовые акты в области информационной безопасности; – правила проведения возможных проверок; – этапы определения конфиденциальности документов объекта защиты; – структуру систем условного доступа и принцип их работы; – 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

2.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 382 часа, в том числе:

на освоение МДК - 310 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося– 208 часов;

самостоятельной работы обучающегося– 102 часа;

на практики: производственную –72 часа.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

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								Учебная, часов	Производственная часов
			Всего, часов	теоретическое	практические занятия,	лабораторные занятия, часов	в т.ч., курсовая работа (проект), часов	Самостоятельная работа обучающегося, часов	консультации часов	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11	12	13
ПК 3.1-3.3 ОК 1-9	МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и радиовещания	156	104	62	-	42	-	52	-	-	-	72 (2 нед)
ПК 3.1-3.3 ОК 1-9	МДК.03.02 Технология использования систем условного доступа в сетях вещания	154	104	60	-	44	-	50	-	-		
ПК 3.1-3.3 ОК 1-9	Производственная практика	72	-	-	-	-	-	-	-	-		
Всего:		382	208	122	-	86	-	102	-	-	-	72

3.2. Тематический план и содержание профессионального модуля ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания

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
МДК.03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и радиовещания			156
Тема 1.1. Основы информационной безопасности	Содержание учебного материала		20
	1	Понятие информационной безопасности, характеристика ее составляющих. Место информационной безопасности в системе национальной безопасности.	
	2	Концептуальная модель защиты информации. Проблемы информационной безопасности в сфере телекоммуникаций: объекты защиты; виды защиты; системы защиты информации.	
	3	Классификация и анализ угроз информационной безопасности в телекоммуникационных системах. Виды уязвимости информации и формы ее проявления.	
	4	Понятие о конфиденциальной информации (грифы, закон о государственной тайне, закон о личной тайне, закон о коммерческой тайне).	
	5	Уровни информационной безопасности – законодательно-правовой, административно-организационный, программно-технический. Принципы построения систем защиты информации.	
	Лабораторные занятия		10
	1	Защита и обработка конфиденциальной документации.	
	2	Организация аттестации выделенного помещения по требованиям ФСТЭК.	
Тема 1.2 Правовое обеспечение информационной безопасности	Содержание учебного материала		20
	1	Информация как объект права. Нормативно-правовые основы информационной безопасности в РФ.	
	2	Законодательно - нормативные акты в области обеспечения информационной безопасности, защиты государственной тайны и конфиденциальной информации.	
	3	Конституционные гарантии прав граждан в области информационной безопасности. Понятие и виды защищаемой информации по законодательству РФ.	
	4	Система защиты государственной тайны, правовой режим защиты государственной тайны.	
	5	Лицензирование и сертификация в области защиты информации. Стандартизация	

		информационной безопасности.	12
	Лабораторные занятия		
	1	Изучение мировых стандартов по защите информации.	
	2	Исследование системы анализа рисков и проверки политики информационной безопасности предприятия.	
Тема 1.3 Организационное обеспечение информационной безопасности	Содержание учебного материала		22
	1	Сущность и сферы действия организационной защиты информации.	
	2	Механизмы обеспечения информационной безопасности. Разработка политики безопасности.	
	3	Проведение анализа угроз и расчета рисков в области информационной безопасности.	
	4	Выбор механизмов и средств обеспечения информационной безопасности. Модели защиты информационных систем.	
	5	Правила организации работ подразделений защиты информации. Разработка инструкций по работе со средствами защиты.	
	6	Организация работы персонала с конфиденциальной информацией.	20
	Лабораторные занятия		
	1	Анализ информационных рисков предприятия.	
	2	Разработка положений о защите персональных данных работников предприятий.	
	3	Разработка политики безопасности предприятия.	52
	Самостоятельная работа обучающихся по МДК.03.01		
	1	1. Оформление в виде конспекта основных руководящих документов об автоматизированных системах. 2. Разработка схемы классификации автоматизированных систем. 3. Изучение концепции автоматизированной системы. 4. Составление схемы подсистема защиты от несанкционированного доступа. 6. Разработка схемы Парольной аутентификации. 7. Оформление в виде конспекта основных положений общеметодологических принципов формирования теории защиты. 8. Составление перечня задач теории защиты. 9. Принципы построения защиты в сетях 10. Оформление в виде конспекта вопросов, касающихся понятия стратегии защиты информации и особенностей стратегических решений. 11. Подготовка перечня требований к сервисам безопасности. 12. Составление схемы основных составляющих политики безопасности. 13. Оформление в виде конспекта основных положений Механизма аутентификации.	

		<p>14. Разработка структуры процессов технологии управления подсистемой защиты ОС.</p> <p>15. Понятие системного анализа: микроскопическое представление системы, иерархическое представление системы.</p> <p>16. Разработка классификации моделей защиты.</p> <p>17. Оформление в виде конспекта основных требований к Средствам и методам выявления компьютерных вирусов.</p> <p>18. Подготовка архитектурной модели Управления доступом.</p> <p>19. Оформление в виде конспекта основных положений Аутентификации в доменах Windows.</p> <p>20. Составление перечня стадий Сетевых атак.</p> <p>21. Определение типовой модели системы автоматизированного проектирования защиты информации.</p> <p>22. Разработка модели защиты информации.</p> <p>23. Оформление в виде конспекта основных положений аппаратных средств защиты информации.</p> <p>24. Оформление в виде конспекта основных видов контроля безопасности.</p> <p>25. Подготовка плана Аудита. Оформление в виде конспекта основных положений математической защиты информации.</p> <p>26. Составление перечня методов кодирования информации.</p> <p>27. Разработка алгоритма хеширования.</p> <p>28. Подготовка перечня антивирусных программ.</p> <p>29. Оформление в виде конспекта основных положений инженерно-технической защиты информации.</p> <p>30. Разработка схемы защиты операционной системы.</p> <p>31. Оформление в виде конспекта основных видов потенциально опасных программ.</p>	
МДК.03.02 Технология использования систем условного доступа в сетях вещания			154
Тема 2.1 Программно-аппаратные средства защиты информации	Содержание учебного материала		24
	1	Информационная безопасность в телекоммуникационных и информационно-коммуникационных сетях.	
	2	Структурные схемы систем защиты информации в типовых информационных системах. Показатели защищенности телекоммуникационных систем.	
	3	Сервисы, обеспечивающие информационную безопасность в многоканальных телекоммуникационных системах и сетях электросвязи: ограничение физического доступа к автоматизированным системам; идентификация и аутентификация пользователей; ограничение доступа в систему; разграничение доступа; регистрация событий (аудит).	

	4	Криптографическая защита; контроль целостности; управление политиками безопасности; уничтожение остаточной информации; резервирование данных; сетевая защита; защита от утечки и перехвата информации по техническим каналам. Подсистемы безопасности.	
	5	Типовые удаленные сетевые атаки и их характеристика. Компьютерные вирусы и защита от них. Антивирусные программы и комплексы.	
	6	Построение систем антивирусной защиты телекоммуникационных систем и сетей.	
	Лабораторные занятия		22
	1	Методы защиты информации. Шифр простой перестановки.	
	2	Методы защиты информации. Шифр Цезаря.	
	3	Резервное копирование информации.	
	4	Основные признаки присутствия на компьютере вредоносных программ.	
	5	Взлом моноалфавитного подстановочного шифра методом частотной атаки.	
	6	Одноразовые блокноты.	
	7	Сеть Фейштеля.	
	8	Шифрование с открытым ключом и электронная цифровая подпись на GPG. Метод шифрования с открытым ключом RSA.	
	9	Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.	
Тема 2.2 Администрирование телекоммуникационных систем и сетей связи	Содержание учебного материала		36
	1	Технологии защиты данных. Принципы криптографической защиты информации (симметричные и асимметричные алгоритмы шифрования, электронная цифровая подпись, стеганография).	
	2	Различные технологии аутентификации. Технологии защиты межсетевого обмена данных. Технология обеспечения безопасности сетевых операционных систем. Основы технологии виртуальных защищенных сетей VPN.	
	3	Технология обнаружения вторжений (анализ защищенности и обнаружения сетевых атак). Требования по защите от несанкционированного доступа Технические средства обеспечения безопасности многоканальных телекоммуникационных систем.	
	4	Многоуровневая защита корпоративных сетей. Режим функционирования межсетевых экранов и их основные компоненты. Маршрутизаторы. Шлюзы сетевого уровня. Усиленная аутентификация. Основные схемы сетевой защиты на базе межсетевых экранов. Применение межсетевых экранов для организации виртуальных корпоративных сетей. Программные методы защиты информации. Защита компьютерных систем от удаленных атак через сеть Internet.	
	5	Классификация способов защиты информации в компьютерных сетях. Понятие разрушающего программного воздействия. Модели взаимодействия прикладной	

		программы и программной закладки. Методы перехвата и навязывания информации. Методы внедрения программных закладок.	
	6	Компьютерные вирусы как особый класс разрушающих программных воздействия. Защита от разрушающих программных воздействий. Антивирусная защита в сетях. Понятие изолированной программной среды. Рекомендации по защите информации Internet.	
	7	Организационные требования к системам информационной защиты ИС. Требования по обеспечению информационной безопасности к аппаратным средствам и программному обеспечению. Требования по применению способов, методов и средств защиты информации. Требования к документированию событий в системе и выявлению несанкционированного доступа. Организация аудита информационной безопасности ИС и предприятия в целом.	
	Лабораторные занятия		22
	1	Виды и конфигурирования VPN-туннелей.	
	2	Технические средства обнаружения, локализации и нейтрализации радиоизлучающих специальных технических средств негласного получения информации.	
	3	Исследование защищенности беспроводных сетей передачи данных.	
	4	Программные средства анализа сетей с коммутацией пакетов. Анализ сетевого трафика с помощью программы «Wireshark».	
	5	Скрытая передача информации в JPEG изображениях.	
	6	Исследование и администрирование средств обеспечения информационной безопасности Microsoft ISA Security Server. Установка и конфигурирование брандмауэра ISA. Построение VPN-сети на базе ISA.	
	7	Многофункциональный поисковый прибор ST-031 «Пиранья». Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ-МИНИ».	
	8	Организация инженерно-технической защиты информации.	
	Самостоятельная работа обучающихся по МДК.03.02		50
	1	1. Оформление в виде конспекта основных положений криптографии. 2. Разработка схемы Механизма арбитраж. 3. Изучение структуры Симметричной системы шифрования. 4. Составление схемы сервера приложений. 5. Оформление в виде конспекта основных положений процесса генерации ключей. 6. Подготовка схемы Абонентское шифрование. 7. Разработка схемы Пакетное шифрование.	

	<p>8. Разработка схемы Аутентификация данных .</p> <p>9. Оформление в виде конспекта основных положений представления алфавита в двоичном коде .</p> <p>10. Подготовка схемы функционирования электронных платежных систем.</p> <p>11. Оформление в виде конспекта основ кодирования.</p> <p>12. Разработка схемы Однонаправленных хеш-функций.</p> <p>13. Разработка схемы шифрования с открытым ключом.</p> <p>14. Оформление в виде конспекта материала по Шифрованию методами замены.</p> <p>15. Оформление в виде конспекта материала об Абонентском шифровании.</p> <p>16. Разработка схемы Матричной перестановки.</p> <p>17. Оформление в виде конспекта материала о криптоанализе.</p> <p>18. Подготовка к практическому занятию «Кодирование».</p> <p>19. Разработка схемы Частотного анализа.</p> <p>20. Разработка схемы криптоанализа.</p> <p>21. Подготовка к практическому занятию «Простая замена».</p> <p>22. Оформление в виде конспекта материала о Компьютерном шифровании.</p> <p>23. Оформление в виде конспекта материала о Гаммировании.</p> <p>24. Подготовка к практическому занятию «Протоколы управления маршрутизацией».</p> <p>25. Подготовка материала о криптографических протоколах.</p> <p>26. Подготовка к практическому занятию «Абсолютный шифр. Шифроблокнот».</p> <p>27. Подготовка материала о Таблице Виженера.</p> <p>28. Поиск и оформление в виде конспекта материалов по теме «Персональный идентификационный номер»</p> <p>29. Разработка структуры генерации ключей.</p> <p>30. Оформление в виде конспекта материала о Структурной схеме шифрования с открытым ключом.</p>	
<p>Производственная практика: Виды работ:</p> <ol style="list-style-type: none"> 1. Исследование детектора электромагнитного поля ST107. 2. Нелинейный локатор SEL SP-61 «Катран». 3. Технические средства защиты информации в телефонных линиях. 4. Контроль эффективности защиты речевой информации с помощью программно-аппаратного комплекса «СПРУТ-МИНИ». 5. Запись и чтение информации для пластиковых карт с магнитной полосой. 6. Исследование и администрирование средств обеспечения информационной безопасности Web-сервера Microsoft IIS Server. 7. Исследование и развертывание сетевой инфраструктуры Microsoft Windows Exchange Server. 		72

- | | |
|--|--|
| <ol style="list-style-type: none">8. Диагностика сетевых подключений с помощью встроенных утилит операционной системы.9. Microsoft Windows.10. Определение среднего коэффициента загрузки дуплексного канала передачи на реальной сети Fast Ethernet с помощью пакетного анализатора.11. Wireshark: выделение ключевых кадров, сохранение данных захвата, просмотр кадра в отдельном окне, печать.12. Wireshark: анализ протоколов Ethernet и ARP.13. Wireshark: анализ протоколов IP и ICMP.14. Wireshark : анализ протокола TCP.15. Работа на оборудовании объединенных сетей по обеспечению защиты информации.16. Администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.17. Настройка и конфигурирование VPN-туннелей L2, IP SEC L3, защищенные приложения L4 SSL, SSH.Аутентификация и идентификация с использованием сетевых операционных систем.19. Установка, настройка специализированного оборудования по защите информации.20. Выявление возможных атак на автоматизированные системы.21. Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей.22. Конфигурирование автоматизированных систем и информационно-коммуникационных сетей.23. Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей.24. Организации защиты в различных операционных системах и средах. | |
|--|--|

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение профессионального модуля

Кабинет компьютерного моделирования

Комплект мебели для учебного процесса.

Мультимедийное оборудование: компьютеры – 12 шт.: ПК 3 - ICL RAY S902.3, монитор ViewSonic VA2038W-LED; монитор 19" ViewSonic TFT 19" VA916; систем. блок P-Athlon64 X2 6000/1024*2М6/320 Gb/клавиатура+мышь+коврик; сканер MUSTEK Bear Paw 2400; прин-тер Canon LBP-1120; проектор мультимедийный Hitachi; калькуляторы.

Программное обеспечение: 1С: Документооборот 8 КОРП (лицензия №75027601); 1С:Предприятие 8. Комплект для обучения (лицензия №8922961); 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); Агент Dr.Web (лицензия № QS34-NC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); комплект ПО для решения основных пользовательских задач (свободно распр. ПО); справочная правовая система «Консультант Плюс» (контракт №2023_СВ_3 от 29.12.2022г); КОМПАС-3D V19 (лицензия №Вг-20-00154); LABVIEW (лицензия №M75X89867); Мой Офис Образование (договор № 2350/2017).

Средства обучения: учебная доска, справочные пособия и дидактический материал, медиатека (мультимедиа разработки и презентации к урокам), экран.

Лаборатория информационной безопасности телекоммуникационных систем

Комплект мебели для учебного процесса.

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

Программное обеспечение: 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); анти-вирусный программный комплекс: Агент Dr.Web (лицензия № QS34-NC7C-SD53-K5L2); ком-плект 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_СВ_3 от 29.12.2022г); программные средства выявления уязвимостей в АС и СБТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО), Metasploit Framework (сво-бодно распр. ПО); программные средства криптографической защиты информации (Крипто-Про 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).

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; многофункциональный поисковый прибор ST 031; нелинейный локатор 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 Е, 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-Cart 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.

Лаборатория телекоммуникационных систем

Комплект мебели для учебного процесса.

Мультимедийное оборудование: системный блок CEL D-341 FAN/ASUS S-775/512 M/160.0G/DVD+-RW; антенна M102 в компл. с кабелем ВЧ TNCm-SMAm; антенный коммута-тор RK-318+RU-005A; внешний накопитель флешка USB TRANSCEND Jetflash 780 64 Gb; Монитор 19"Samsung 940N (LKSB) TFT, 2 шт.; МФУ 3210V_N Xerox Work Centre 3210; МФУ Canon Laser Base MF 3228 (копир.принтер.сканер) A4; ноутбук Dell Latitude E6520 Intel Core I5 Processor 2520M 15,6", 2 шт.; ноутбук Samsung NP -RF 511-S02RU 15,6"; ПК S404,2 400W/Intel Core i3 540/клав.,мышь,монит. 21,5" VA2248-LED; ПК H404,2 420W/Intel Core i3 540/клав.,мышь,монит. 21,5" VA2248-LED, 2 шт.; приемник IC-R75; систем.блок АМД3000+(512*2)/160Gb/DVD+RWrkfd/+мышь+коврик+клавав.

Программное обеспечение: 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); Агент Dr.Web (лицензия № QS34-HC7C-SD53-K5L2); комплект ГАРАНТ–Мастер (лицензия №12–40272–000898); Комплект ПО для решения основных пользовательских задач (свободно распространяемое ПО); справочная правовая система «Консультант Плюс» (контракт №2023_СВ_3 от 29.12.2022г).

Средства обучения: кварцевый генератор "Астра" 10 МГц; комплекс лабораторного оборудования "Программируемая платформа для ВЧ-приложений" для работы в диапазоне частот 1-250МГц; лабораторный комплект по цифровой обработке сигналов; система сбора и анализа данных и управления; стандарт частоты GPS-12 RG в комплекте с антенной ACM-03 и кабелем; телевизор LED 42" LG 42LS; точка доступа Cisco AIR-CAP 1602I-R-K9; универсальная приёмо-передающая платформа для проектирования СВЧ-систем компл.mgxc2; устройство частотно времен-ной синхронизации по сигналам СНС ГЛОНАС и GPS NAVSTAR СН-3833; учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети); учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети) ; экран на штативе 180x180 см., управляемый коммутатор L2-2 шт., управляемый межсетевой экран-маршрутизатор L3-2 шт., комплект SFP-модулей FTTx для коммутаторов и маршрутизаторов, конвертеры 2 шт., мультиплексоры 2 шт., комплекты пассивных элементов для подключения абонентских терминалов и выполнения кроссировки, набор инструментов для выполнения кроссировочных работ.

Договоры о практической подготовке:

АО «Марийский машиностроительный завод» Договор № 1/2021 от 01.02.2021 – бессрочный.

Филиал ПАО «Ростелеком» в Республике Марий Эл Договор № 83/2021 от 27.01.2021 - бессрочный.

4.2. Информационное обеспечение профессионального модуля

Основная и дополнительная литература

№ п/п	Список используемой литературы (<i>печатные издания, электронные издания за последние 5 лет</i>)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
ОСНОВНАЯ ЛИТЕРАТУРА		
1.	Гилязова, Р.Н. 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: https://e.lanbook.com/book/173796 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.	электронный ресурс
2.	Никифоров, С.Н. 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: https://e.lanbook.com/book/146802 (дата обращения: 27.11.2020). — Режим доступа: для авториз. пользователей.	электронный ресурс
3.	Организационно-техническое и правовое обеспечение информационной безопасности Российской Федерации: 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: https://znanium.com/catalog/product/1999941 (дата обращения: 29.08.2023). – Режим доступа: по подписке. https://znanium.com/catalog/document?id=426504#bib	электронный ресурс
4.	Хорев, П.Б. Программно-аппаратная защита информации: учебное пособие / П.Б. Хорев. - 2-е изд., испр. и доп. - Москва: ФОРУМ: ИНФРА-М, 2021. - 352 с. - (Среднее профессиональное образование) - https://znanium.com/read?id=364477	электронный ресурс
ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА		
	Учебники, учебные пособия	
1.	Ищейнов, В.Я. Основные положения информационной безопасности: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - Москва: ФОРУМ: ИНФРА-М, 2021. - 208 с. - (Среднее профессиональное образование) - https://znanium.com/read?id=365084	электронный ресурс
2.	Петренко, В.И. 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: https://e.lanbook.com/book/153678 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.	электронный ресурс

3.	<p>Прохорова, О.В. 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: https://e.lanbook.com/book/158939 (дата обращения: 16.11.2021). — Режим доступа: для авториз. пользователей.</p>	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 - дифференцированный зачет, 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 лабораторных работ.

№	Наименование темы	Код формируемой компетенции	Результаты обучения по профессиональному модулю		Формы контроля
			уметь	знать	
МДК 03.01 Технология применения комплексной системы защиты информации в системах радиосвязи и радиовещания					
1.	Основы информационной безопасности	ПК 3.1-3.3 ОК 1-9	– классифицировать угрозы информационной безопасности;	– каналы утечки информации; – назначение, классификацию и принципы работы специализированного оборудования; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; – структуру систем условного доступа и принцип их работы; – возможные способы, места установки и настройки программных продуктов; – конфигурации защищаемых сетей; – алгоритмы работы тестовых программ;	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практическом обучении. Экзамен (квалификационный) по профессиональному модулю.
2.	Правовое обеспечение информационной безопасности	ПК 3.1-3.3 ОК 1-9	– классифицировать угрозы информационной безопасности; – определять возможные виды атак; – использовать программные продукты, выявляющие недостатки систем защиты; – использовать программные продукты для защиты баз данных;	– законодательные и нормативные правовые акты в области информационной безопасности; – правила проведения возможных проверок;	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на

					практическом обучении. Экзамен (квалификационный) по профессиональному модулю.
3.	Организационное обеспечение информационной безопасности	ПК 3.1-3.3 ОК 1-9	<ul style="list-style-type: none"> – классифицировать угрозы информационной безопасности; – использовать программные продукты, выявляющие недостатки систем защиты; 	<ul style="list-style-type: none"> – каналы утечки информации; – назначение, классификацию и принципы работы специализированного оборудования; – возможные способы несанкционированного доступа; – этапы определения конфиденциальности документов объекта защиты; – алгоритмы работы тестовых программ; 	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практическом обучении. Экзамен (квалификационный) по профессиональному модулю.

МДК 03.02 Технология использования систем условного доступа в сетях вещания

1	Программно-аппаратные средства защиты информации	ПК 3.1-3.3 ОК 1-9	<ul style="list-style-type: none"> – определять возможные виды атак; – использовать программные продукты, выявляющие недостатки систем защиты; – выполнять тестирование систем с целью определения уровня 	<ul style="list-style-type: none"> – каналы утечки информации; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; 	Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка
---	--	----------------------	--	---	---

			<p>защищенности;</p> <ul style="list-style-type: none"> – использовать программные продукты для защиты баз данных; 	<ul style="list-style-type: none"> – правила проведения возможных проверок; – структуру систем условного доступа и принцип их работы; – алгоритмы работы тестовых программ; – собственные средства защиты различных операционных систем и сред; - способы и методы шифрования информации 	<p>решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практическом обучении.</p> <p>Экзамен (квалификационный) по профессиональному модулю.</p>
2	Администрирование телекоммуникационных систем и сетей связи	ПК 3.1-3.3 ОК 1-9	<ul style="list-style-type: none"> – определять возможные виды атак; – осуществлять мероприятия по проведению аттестационных работ; – разрабатывать политику безопасности объекта; – выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта; – использовать программные продукты, выявляющие недостатки систем защиты; – производить установку и настройку средств защиты; – конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; – выполнять тестирование систем с целью определения уровня 	<ul style="list-style-type: none"> – назначение, классификацию и принципы работы специализированного оборудования; – принципы построения информационно-коммуникационных сетей; – возможные способы несанкционированного доступа; – законодательные и нормативные правовые акты в области информационной безопасности; – правила проведения возможных проверок; – этапы определения конфиденциальности документов объекта защиты; – структуру систем условного доступа и принцип их работы; – возможные способы, места установки и настройки программных продуктов; 	<p>Тестирование, экспертное наблюдение выполнения лабораторных работ, оценка решения ситуационных задач, оценка процесса и результатов выполнения видов работ на практическом обучении.</p> <p>Экзамен (квалификационный) по профессиональному модулю.</p>

			<p>защищенности;</p> <ul style="list-style-type: none"> – использовать программные продукты для защиты баз данных; применять криптографические методы защиты информации 	<ul style="list-style-type: none"> – конфигурации защищаемых сетей; – алгоритмы работы тестовых программ; – собственные средства защиты различных операционных систем и сред; способы и методы шифрования информации 	
--	--	--	---	--	--

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 дифференцированного зачета, 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 2023-2024 учебный год по профессиональному модулю ПМ.03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания: в раздел Условия реализации учебной дисциплины (пункт Информационное обеспечение учебной дисциплины) внесены изменения в список основной и дополнительной литературы.

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

«30» августа 2023 г. (протокол № 1)

Председатель ПЦК  /Кузнецов Е.Ю./

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 в телекоммуникационных системах и сетях вещания: 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./