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 ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

по специальности 11.02.15 Инфокоммуникационные сети и системы связи

2022

РАССМОТРЕНА И ОДОБРЕНА
Предметно-цикловой комиссией
Протокол № 5
«28» апреля 2022 г.
Председатель ПЦК _____ /Кузнецов Е.Ю./

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи разработана на основе Федерального государственного образовательного стандарта по специальности *11.02.15 Инфокоммуникационные сети и системы связи*.

Организация-разработчик: Высший колледж ПГТУ «Политехник».

Разработчик:
Савинов Александр Николаевич, канд. техн. наук, доцент кафедры информационно-вычислительных систем ФГБОУ ВО «ПГТУ».

Рецензент (внутренний)
Кузнецов Е.Ю., преподаватель с ученой степенью кандидата технических наук, заместитель директора по УМР Высшего колледжа «Политехник».
Рецензент (внешний)
Ерасланов С.Г., директор сервисного центра г. Йошкар-Ола филиала Республики Марий Эл ПАО «Ростелеком».

©Савинов А.Н., 2022

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 инфокоммуникационных сетей и систем связи относится к профессиональному циклу по программе подготовки специалистов среднего звена, устанавливающей базовые знания по специальности среднего профессионального образования 11.02.15 Инфокоммуникационные сети и системы связи.

Общий объем учебной нагрузки по профессиональному модулю составляет 647 часов, нагрузка во взаимодействии с преподавателем составляет 354 часа, часов самостоятельной работы – 95.

Содержание профессионального модуля включает:

- изучение разделов междисциплинарного курса МДК 03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи:

1. Основы безопасности информационных технологий
2. Обеспечение безопасности информационных технологий
3. Средства защиты информации от несанкционированного доступа.
4. Обеспечение безопасности компьютерных систем и сетей.

- изучение разделов междисциплинарного курса МДК.03.02. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи:

1. Основы информационной безопасности.
2. Организационно-правовые аспекты защиты информации.
3. Комплексная система защиты информации.
4. Инженерно-техническая защита информации.
5. Криптографическая защита информации
6. Аттестация и лицензирование объектов защиты.

Текущий контроль проводится в форме оценки тестирования, экспертного наблюдения за выполнением лабораторных 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 инфокоммуникационных сетей и систем связи относится к профессиональному учебному циклу профессиональной подготовки программы подготовки специалистов среднего звена по специальности среднего профессионального образования *11.02.15 Инфокоммуникационные сети и системы связи*.

2.2. Цель и планируемые результаты освоения профессионального модуля

В результате освоения профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи обучающийся должен обладать предусмотренными ФГОС СПО по специальности *11.02.15 Инфокоммуникационные сети и системы связи* умениями, знаниями, которые формируют следующие **профессиональные компетенции:**

Код	Наименование результата обучения
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 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.

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

Код	Наименование результата обучения
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.
ОК 09	Использовать информационные технологии в профессиональной деятельности.
ОК 10	Пользоваться профессиональной документацией на государственном и иностранном

	языках.

Результаты обучения (знания, умения, практический опыт)

В результате освоения профессионального модуля обучающийся должен:

иметь практический опыт	– выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности; – разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; – осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
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.

2.3. Количество часов, отводимое на освоение профессионального модуля:

Всего часов – 647 часов, в том числе:
на освоение МДК - 449 часов, включая:
обязательной аудиторной учебной нагрузки обучающегося–354 часа;
самостоятельной работы обучающегося– 95 часов;
на практики: учебную – 72 часа,
производственную –108 часов;
экзамен (квалификационный) – 18 часов.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

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	курсовая работа (проект), часов					
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
ПК 3.1, 3.3 ОК 01-10	МДК.03.01. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.	**225**	**174**	**70**	**-**	**104**	**-**	**51**	**-**	**-**	**72 (2 нед)**	**108 (3 нед)**
ПК 3.1-3.3 ОК 01-10	МДК.03.02. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.	**224**	**180**	**90**	**-**	**90**	**-**	**44**	**-**	**-**		
ПК 3.1-3.3 ОК 01-10	Учебная практика	**72**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**		
	Производственная практика	**108**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**-**		
	Экзамен (квалификационный)	**18**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**18**		
	Всего:	**647**	**354**	**160**	**-**	**194**	**-**	**95**	**-**	**18**	**72**	**108**

3.2. Тематический план и содержание профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

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. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.			**225**
Тема 1.1. Основы безопасности информационных технологий.	**Содержание учебного материала**		16
	1	Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами.	
	2	Основные понятия в области безопасности информационных технологий. Информация и информационные отношения.	
	3	Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем.	
	4	Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности.	
	5	Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация.	
	6	Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи.	
	7	Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей.	
	Лабораторные занятия		28
	1	Сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	
	2	Получение списка пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	
	3	Создание отчетов на базе СПО ЗИ (например, РЕВИЗОР-1XP).	
	4	Установка прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	
	5	Считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	
	6	Сканирования дерева ресурсов с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	
	7	Регистрация пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP).	

	Самостоятельная работа обучающихся		18
	1	Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	
	2	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	
Тема 1.2. Обеспечение безопасности информационных технологий.	**Содержание учебного материала**		20
	1	Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций.	
	2	Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников.	
	3	Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты.	
	4	Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников.	
	5	Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы.	
	6	Регламентация процессов разработки, внедрения и сопровождения задач.	
	7	Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов.	
	8	Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы.	
	9	Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности.	
	10	Концепция безопасности информационных технологий предприятия. Назначение и статус документа.	
	Лабораторные занятия		20
	1	Установка и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT).	
	2	Исследование программной среды с помощью СЗИ НСД (например, Страж NT).	
	3	Исследование возможностей управления пользователями с помощью СЗИ НСД (например, Страж NT).	
	4	Исследование учета пользователей и контроля устройств с помощью СЗИ НСД (например, Страж NT).	
	5	Исследование избирательного управления с помощью СЗИ НСД (например, Страж	

		NT).	
	6	Исследование сортировки и поиска с помощью СЗИ НСД (например, Страж NT).	
	7	Исследование возможности редактирования пользователей с помощью СЗИ НСД (например, Страж NT).	
	8	Исследование изменения настроек СЗИ с помощью СЗИ НСД (например, Страж NT).	
	9	Исследование механизма защиты съемных носителей с помощью СЗИ НСД (например, Страж NT).	
	10	Исследование настройки маркировки документов с помощью СЗИ НСД (например, Страж NT).	
	Самостоятельная работа обучающихся		18
	1	Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы.	
	2	Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации.	
Тема 1.3. Средства защиты информации от несанкционированного доступа.	**Содержание учебного материала**		20
	1	Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц.	
	2	Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем.	
	3	Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK).	
	4	Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть»).	
	5	Назначение и особенности применения СЗИ НСД (например, «Страж NT»).	
	6	Назначение и специфика применения комплекса ЗИ (например, «Соболь»).	
	7	Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей.	
	8	Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи-Хеллмана.	
	9	Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа.	
	Лабораторные занятия		36

	1	Ввод информации в САПР СЗИ (например, «Гроза-К»).	
	2	Расчет радиуса контролируемой зоны с помощью САПР СЗИ (например, «Гроза-К»).	
	3	Исследование защищенности с помощью САПР СЗИ (например, «Гроза-К»).	
	4	Формирование и вывод проекта протокола в САПР СЗИ (например, «Гроза-К»).	
	5	Исследование плана тестирования при помощи СПО ЗИ (например, «Ревизор-2XP»).	
	6	Исследование режима тестирования при помощи СПО ЗИ (например, «Ревизор-2XP»).	
	7	Исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»).	
	8	Исследование механизма доступа в систему с использованием СПО ЗИ и УП (например, «SecretNet»).	
	9	Исследование механизма разграничения доступа с использованием СПО ЗИ и УП (например, «SecretNet»).	
	Самостоятельная работа обучающихся		15
	1	Самостоятельное изучение постановлений правительства, законов и других руководящих документов в области защиты информации.	
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей.	**Содержание учебного материала**		14
	1	Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративная сеть. Уязвимости и их классификация.	
	2	Назначение, возможности и защитные механизмы межсетевых экранов. Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов.	
	3	Анализ содержимого почтового и WEB-трафика. HTTP-трафик.	
	4	Виртуальные частные сети. Решение на базе ОС Windows 2003. VPN на основе криптошлюза (например, «Континент-К»).	
	5	Обнаружение и устранение уязвимостей. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования.	
	6	Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий.	
	Лабораторные занятия		20
	1	Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП (например, «SecretNet»).	
	2	Исследование функции отслеживания событий НСД с использованием СПО ЗИ и	

		УП (например, «SecretNet»).	
	3	Исследование возможности обновления клиента с использованием СПО ЗИ и УП (например, «SecretNet»).	
	4	Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»).	
	5	Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например, «SecretNet»).	
МДК.03.02. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.			**224**
Тема 2.1. Основы информационной безопасности.	**Содержание учебного материала**		12
	1	Основные понятия информационной безопасности. Сущность и понятия защиты информации.	
	2	Значение информационной безопасности и ее место в системе национальной безопасности.	
	3	Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	
	4	Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации.	
	5	Состояние информационной безопасности РФ и основные задачи по ее обеспечению.	
	6	Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности.	
	Лабораторные занятия		14
	1	Исследование возможностей профессионального нелинейного радиолокатора (например, NR-900EMS).	
	2	Исследование возможностей многофункционального поискового прибора (например, ST 033P Пиранья).	
	3	Исследование возможностей анализатора спектра (например, OSCORGreen-8).	
	4	Исследование возможностей имитатора источника радиосигналов с различными видами модуляции (например, АВРОРА-3).	
	5	Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО).	
	Самостоятельная работа обучающихся		8
	1	Изучение основополагающих документов, затрагивающих интересы РФ в	

		информационной сфере.	
	2	Ознакомление с нормативными документами.	
Тема 2.2. Организационно-правовые аспекты защиты информации.	**Содержание учебного материала**		10
	1	Структура правовой защиты информации. Система документов в области защиты информации.	
	2	Организационные основы защиты информации. Принципы организационной защиты информации.	
	3	Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации.	
	4	Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности.	
	5	Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере.	
	Лабораторные занятия		16
	1	Исследование возможностей скоростного приемника сигналов (например, СКОРПИОН-XL).	
	2	Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).	
	3	Исследование возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Ф и ФСП-1Ф-10А).	
	4	Исследование работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501).	
	Самостоятельная работа обучающихся		4
	1	Подготовка презентации по заданной теме с последующим представлением преподавателю в электронном виде.	
Тема 2.3. Комплексная система защиты информации.	**Содержание учебного материала**		10
	1	Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации.	
	2	Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна.	
	3	Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны.	

	4	Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение.	
	5	Способы и средства обнаружения угроз. Комплексное обследования защищенности информационной системы. Средства нейтрализации угроз.	
	Лабораторные занятия		16
	1	Исследование уязвимостей и построение модели угроз объекта защиты.	
	2	Разработка комплексной системы инженерно-технической защиты информации на объекте.	
	3	Исследование возможностей устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б).	
	4	Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств (например, ПРОКРУСТ-2000).	
	Самостоятельная работа обучающихся		6
	1	Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности.	
	2	Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе.	
Тема 2.4. Инженерно-техническая защита информации.	**Содержание учебного материала**		30
	1	Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.	
	2	Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации.	
	3	Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации.	
	4	Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации.	
	5	Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД.	
	6	Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению.	
	7	Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи.	
	8	Акустический контроль. Понятие разборчивости речи при перехвате информации.	

		Способы и средства информационного скрытия речевой информации от подслушивания.	
	9	Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок.	
	10	Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания.	
	11	Контроль слаботочных цепей. Принципы контроля линий заземления.	
	12	Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации.	
	13	Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники.	
	Лабораторные занятия		26
	1	Исследование возможностей автоматизированной системы изменений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ).	
	2	Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ).	
	3	Исследование возможностей системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ).	
	4	Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ).	
	5	Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи (например, ЛАЗУРИТ).	
	6	Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН (например, СИГУРД-М19).	
	7	Оценка защищённости с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН (например, СИГУРД-М19).	
	8	Измерение параметров ПЭМИН и расчет показателей защищенности технического средства (например, с помощью комплекса СИГУРД-М19).	
	9	Исследование возможностей системы оценки защищенности выделенных помещений (например, ШЕПОТ).	
	10	Измерение уровня звукового давления вблизи и на удалении от источника с	

		помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ).	
	11	Измерение уровня виброускорения в ограждающих конструкциях (например, с помощью комплекса ШЕПОТ).	
	12	Расчет и оценка защищенности помещения по акустическому каналу (например, с помощью комплекса ШЕПОТ).	
	13	Расчет и оценка защищенности помещения по виброакустическому каналу (например, с помощью комплекса ШЕПОТ).	
	Самостоятельная работа обучающихся		10
	1	Разработка пакета документации по инженерно-технической защите информации на объекте.	
	2	Изучение возможностей инженерно-технических средств защиты информации.	
	3	Изучение технических характеристик инженерно-технических средств защиты информации.	
	4	Разработка предложений по инженерно-технической защите информации на определенном объекте.	
	5	Составление доклада по перспективе и направлению развития инженерно-технических средств защиты информации на основе публикаций в периодической специализированной аппаратуре.	
Тема 2.5. Криптографическая защита информации.	**Содержание учебного материала**		16
	1	Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных.	
	2	Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.	
	3	Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом.	
	4	Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи.	
	Лабораторные занятия		12
	1	Поиск и локализация скрытых видеокамер (например, с помощью прибора ОПТИК-2).	
	2	Исследование методов защиты сотовых телефонов от несанкционированного прослушивания (например с помощью изделия Ладья-ИВТ).	
	3	Исследование методов блокирования средств несанкционированного	

		прослушивания и передачи данных различных стандартов (например, с помощью устройства КЕДР-1М).	
	4	Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора (например, с помощью NR-900EMS).	
	5	Поиск устройств негласного съема информации с помощью многофункционального поискового прибора (например, с помощью ST 033P Пиранья).	
	6	Оценка защищенности помещения с помощью многофункционального поискового прибора (например, ST 033P Пиранья).	
	Самостоятельная работа обучающихся		10
	1	Разработка предложений по комплексу технических мероприятий по защите линий связи объекта.	
	2	Разработка предложений по защите информации от несанкционированного доступа по акустическому каналу в помещении.	
Тема 2.6. Аттестация и лицензирование объектов защиты.	**Содержание учебного материала**		12
	1	Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ.	
	2	Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний.	
	3	Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании.	
	Лабораторные занятия		6
	1	Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165).	
	2	Исследование работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221).	
	3	Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО).	
	Самостоятельная работа обучающихся		6
	1	Составление списка уязвимостей предложенного объекта. Самостоятельная разработка комплекта документации на объекте информатизации.	

Учебная практика: **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.	**72**
Производственная практика: **Виды работ:** 1. Участие в создании комплексной системы защиты на предприятии. 2. Применение программно-аппаратных средств защиты информации на предприятии 3. Применение инженерно-технических средств защиты информации на предприятии. 4. Применение криптографических средств защиты информации на предприятии.	**108**
Экзамен (квалификационный)	**18**
ВСЕГО	**647**

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*2Мб/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-HC7C-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 №2025_СВ_2 от 04.12.2024г); 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-HC7C-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 №2025_СВ_2 от 04.12.2024г); программные средства выявления уязвимостей в АС и СВТ (Tenable Nessus® vulnerability scanner (свободно распр. ПО), Metasploit Framework (свободно распр. ПО); программные средства криптографической защиты информации (Крипто-Про CSP 5.0 (лицензионный

контракт №010/IO20-002792 от 28.08.20), ViPNet CSP 4 (свобод-но-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/M «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-аккустической защиты «Соната-АВ»; устройство защиты «Соната-РС2»; 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; антена 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 (ко-пир.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+клвав.

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 En-terprise (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 №2025_СВ_2 от 04.12.2024г).

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 антеной 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 CH-3833; учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети); учебно-научно исслед.комплекс УНИК (Сверхширокополосн. беспроводн.сенсорные сети) ; экран на штативе 180х180 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 (*печатные издания, электронные издания за последние 5 лет*)	Количество экземпляров, имеющихся в библиотеке, или ссылка на ЭБС
	ОСНОВНАЯ ЛИТЕРАТУРА	
1.	**Сергеев, А.А.** Бизнес-планирование: учебник и практикум для среднего профессионального образования/ А.А. Сергеев. — 5-е изд., испр. и доп. — Москва: Издательство Юрайт, 2025. — 435 с. — (Профессиональное образование). — ISBN 978-5-534-20235-9. — Текст: электронный// Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/565767 (дата обращения: 10.06.2025).	электронный ресурс
2.	**Партыка, Т.Л.** Вычислительная техника: учебное пособие / Т.Л. Партыка, И.И. Попов. - 3-е изд., перераб. и доп. - Москва: ФОРУМ: ИНФРА-М, 2022. - 445 с.: ил. - (Среднее профессиональное образование). - ISBN 978-5-00091-510-3. - Текст: электронный. - URL: https://znanium.com/catalog/product/1703191 (дата обращения: 10.09.2023).	электронный ресурс
3.	**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
4.	**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
5.	**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
6.	**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
	ДОПОЛНИТЕЛЬНАЯ ЛИТЕРАТУРА	
	Учебники, учебные пособия	
1.	**Петренко, В.И.** Защита персональных данных в информационных системах. Практикум: учебное пособие для	электронный ресурс

	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.	
2.	**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.	электронный ресурс
3.	**Баранова, Е.К.** Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. - Москва: РИОР: ИНФРА-М, 2022. - 202 с. - (Среднее профессиональное образование). - DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4. - Текст: электронный. - URL: https://znanium.com/catalog/product/1860126 (дата обращения: 21.08.2023).	электронный ресурс
4.	**Ищейнов, В.Я.** Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации: учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - Москва: ИНФРА-М, 2022. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Текст: электронный. - URL: https://znanium.com/catalog/product/1861659 (дата обращения: 21.08.2023).	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 лабораторных работ, 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 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи					
1.	Основы безопасности информационных технологий.	ПК 3.1, 3.3 ОК 01-10	- 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; - 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	- 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; - методы и способы защиты информации, передаваемой по	Тестирование Выполнение лабораторных работ. Экзамен.

			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	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.	
2.	Обеспечение безопасности информационных технологий.	ПК 3.1, 3.3 ОК 01-10	- 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	- 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	Тестирование Выполнение лабораторных работ. Экзамен.

			в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности; - 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	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; - 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.	

3.	Средства защиты информации от несанкционированного доступа.	ПК 3.1, 3.3 ОК 01-10	- 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; - 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	- 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; - 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	Тестирование экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом обучении. Экзамен.

			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	информации; - способы и методы шифрования (кодирование и декодирование) информации.	
4.	Обеспечение безопасности компьютерных систем и сетей.	ПК 3.1, 3.3 ОК 01-10	- 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	- 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	Тестирование экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом обучении. Экзамен.

			защищенности; - 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	радиоканале; - классификацию угроз сетевой безопасности; - характерные особенности сетевых атак; - возможные способы несанкционированного доступа к системам связи; - 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.	
МДК.03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи.					
1.	Основы информационной безопасности.	ПК 3.1, 3.3 ОК 01-10	- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;	- принципы построения информационно-коммуникационных сетей; - международные стандарты	Тестирование экспертное наблюдение выполнения

			- 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; - 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	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; - 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.	лабораторных работ.

			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		
2.	Организационно-правовые аспекты защиты информации.	ПК 3.1, 3.3 ОК 01-10	- 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; - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию,	- 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	Тестирование экспертное наблюдение выполнения лабораторных работ.

			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	атак; - возможные способы несанкционированного доступа к системам связи; - 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.	
3.	Комплексная система защиты информации.	ПК 3.1, 3.3 ОК 01-10	- 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	- 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	Тестирование экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом

			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; - 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	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; - 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.	обучении

			продуктов; - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами		
4.	Инженерно-техническая защита информации.	ПК 3.1, 3.3 ОК 01-10	- 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; - 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	- 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; - методы и способы защиты информации, передаваемой по	Тестирование экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом обучении

			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	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.	
5.	Криптографическая защита информации.	ПК 3.1, 3.3 ОК 01-10	- 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	- 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	Тестирование экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом обучении

			в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности; - 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	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; - 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.	
6.	Аттестация и	ПК 3.1, 3.3	- классифицировать угрозы	- принципы построения	Тестирование

	лицензирование объектов защиты.	ОК 01-10	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; - 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	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; - 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;	экспертное наблюдение выполнения лабораторных работ, оценка процесса и результатов выполнения видов работ на практическом обучении

			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	- способы и методы шифрования (кодирование и декодирование) 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 инфокоммуникационных сетей и систем связи: 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 инфокоммуникационных сетей и систем связи: 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 2024 г. (протокол № 1)

Председатель ПЦК _____ /Кузнецов Е.Ю./

Дополнения и изменения к рабочей программе на учебный год

Дополнения и изменения к рабочей программе на 2025-2026 учебный год по профессиональному модулю ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи: 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 2025 г. (протокол № 1)

Председатель ПЦК _____ /Кузнецов Е.Ю./