ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)
Ярославский филиал ПГУПС**

УТВЕРЖДАЮ
Директор Ярославского филиала ПГУПС
_____ О.М. Епархин
«14» июня 2023 г.

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

**для специальности
11.02.15 Инфокоммуникационные сети и системы связи**

Квалификация **– специалист по монтажу и обслуживанию телекоммуникаций**

Форма обучения – очная

Ярославль
2023

Рассмотрено на заседании ЦК
информационно-коммуникационных
технологий (ИКТ), сетей и систем связи
протокол № 9 от «28» апреля 2023 г.
Председатель_____/Никитин Н.А./

Рабочая программа профессионального модуля ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 11.02.15 Инфокоммуникационные сети и системы связи, утвержденного приказом Министерства просвещения Российской Федерации от 05.08.2022 г. № 675.

Разработчик программы:
Клюев Н.В., преподаватель Ярославского филиала ПГУПС

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

1.1. Область применения рабочей программы

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи в части освоения вида деятельности (ВД): Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и формирования следующих общих компетенций (ОК) и профессиональных компетенций (ПК):

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3.	Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи
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

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

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

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

1.3. Количество часов на освоение рабочей программы профессионального модуля:

Объем образовательной программы обучающегося 424 часов, в том числе:
обязательная часть – 326 часов,
вариативная часть – 98 часов.

Увеличение количества часов рабочей программы за счет часов вариативной части направлено на дальнейшее развитие профессиональных компетенций, расширение объема знаний по разделам программы.

Объем образовательной программы обучающегося 424 часов.
Из них:
на освоение МДК.03.01 – 166 часов, включая самостоятельную работу обучающегося – 14 часов, промежуточную аттестацию в форме экзамена – 6 часов,
из них в форме практической подготовки – 62 часа;
на освоение МДК.03.02 – 138 часов, включая самостоятельную работу обучающегося – 8 часов, промежуточную аттестацию в форме дифференцированных зачетов,
из них в форме практической подготовки – 54 часа;
на производственную практику – 108 часов,
из них в форме практической подготовки – 108 часов.
Экзамен по модулю – 12 часов.

2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения рабочей программы профессионального модуля является овладение обучающимися видом деятельности (ВД): обеспечение информационной безопасности инфокоммуникационных сетей и систем связи, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 3.1.	Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности
ПК 3.2.	Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи
ПК 3.3.	Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования
ОК 01.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 02.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК 04.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 09.	Пользоваться профессиональной документацией на государственном и иностранном языках

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональ-ных и общих компетенций	Наименования разделов профессионального модуля	Суммар-ный объем нагрузки, час.	Объем профессионального модуля, час.							
			Работа обучающихся во взаимодействии с преподавателем, час							Самостоятельная работа
			Обучение по МДК			Практики		Консультации	Промежуточная аттестация	
			Всего	В том числе		Учебная	Производст-венная			
				Лабораторных и практических занятий	Курсовых работ (проектов)					
1	2	3	4	5	6	7	8	9	10	11
ПК 3.1.; ПК 3.3.; ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 09.	Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**166**	**144**	62	-	**-**	**-**	**2**	**6**	**14**
ПК 3.1.; ПК 3.2.; ПК 3.3.; ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 09.	Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	**138**	**130**	54	-	**-**	**-**	**-**	**-**	**8**
ПК 3.1.; ПК 3.2.; ПК 3.3.; ОК 01.; ОК 02.; ОК 03.; ОК 04.; ОК 05.; ОК 06.; ОК 09.	Производственная практика (по профилю специальности), часов	**108**	**-**	-	-	**-**	**108**	**-**	**-**	**-**
	Экзамен по модулю	**12**	**-**	-	-	**-**	**-**	**-**	**12**	**-**
	Всего:	**424**	**274**	**116**	**-**	**-**	**108**	**2**	**18**	**22**

3.2. Тематический план и содержание профессионального модуля (ПМ)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект)	Объем часов
1	2	3
Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**166**
МДК.03.01. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи		**166**
Тема 1.1. Основы безопасности информационных технологий	**Содержание**	**30**
	1. Актуальность проблемы обеспечения безопасности информационных технологий. Место и роль информационных систем в управлении бизнес-процессами. Основные причины обострения проблемы обеспечения безопасности информационных технологий	
	2. Основные понятия в области безопасности информационных технологий. Информация и информационные отношения. Субъекты информационных отношений, их безопасность	
	3. Угрозы безопасности информационных технологий. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности	
	4. Принципы обеспечения безопасности информационных технологий. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты	
	5. Принципы построения системы обеспечения безопасности информации в автоматизированной системе	
	6. Правовые основы обеспечения безопасности информационных технологий. Защищаемая информация	
	7. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры	
	8. Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации	
	9. Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Идентификация и аутентификация пользователей. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности	
	В том числе практических занятий	**12**
	Практическое занятие 1. Сканирование логических дисков с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	Практическое занятие 2. Получение списка пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	Практическое занятие 3. Создание отчетов на базе СПО ЗИ (например, РЕВИЗОР-1XP)	2
	Практическое занятие 4. Установка прав доступа с помощью СПО ЗИ. Считывание прав доступа с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2

	Практическое занятие 5. Сканирования дерева ресурсов с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
	Практическое занятие 6. Регистрация пользователей с помощью СПО ЗИ (например, РЕВИЗОР-1XP)	2
Тема 1.2. Обеспечение безопасности информационных технологий	**Содержание**	**42**
	1. Понятие технологии обеспечения безопасности информации. Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ	
	2. Обязанности пользователей и ответственных за обеспечение безопасности ИТ. Общие правила обеспечения безопасности ИТ при работе сотрудников. Ответственность за нарушения. Порядок работы с носителями ключевой информации	
	3. Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты	
	4. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедура авторизации сотрудников	
	5. Порядок изменения конфигурации программно-аппаратных средств. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация	
	6. Регламентация процессов разработки, внедрения и сопровождения задач. Взаимодействие подразделений на всех этапах внедрения автоматизированных подсистем	
	7. Определение требований к защите и категорирование ресурсов. Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов	
	8. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов	
	9. Планы защиты и планы обеспечения непрерывной работы и восстановления. Составные части планов защиты и обеспечения непрерывной работы	
	10. Средства обеспечения непрерывной работы. Обязанности и действия персонала по обеспечению непрерывной работы	
	11. Основные задачи подразделений обеспечения безопасности ИТ. Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации	
	12. Концепция безопасности информационных технологий предприятия. Назначение и статус документа. Вопросы, которые должны быть отражены в Концепции	
	В том числе практических занятий	**18**
	Практическое занятие 7. Установка и снятие СЗИ с помощью программы СЗИ НСД (например, Страж NT)	2
	Практическое занятие 8. Исследование программной среды с помощью СЗИ НСД (например, Страж NT)	2
	Практическое занятие 9. Исследование возможностей управления пользователями с помощью СЗИ НСД (например, Страж NT)	2
	Практическое занятие 10. Исследование учета пользователей и контроля устройств с помощью СЗИ НСД (например, Страж NT)	2

	Практическое занятие 11. Исследование избирательного управления с помощью СЗИ НСД (например, Страж NT)	2
	Практическое занятие 12. Исследование сортировки и поиска с помощью СЗИ НСД. Исследование возможности редактирования пользователей с помощью СЗИ НСД (например, Страж NT).	2
	Практическое занятие 13. Исследование изменения настроек СЗИ с помощью СЗИ НСД (например, Страж NT)	2
	Практическое занятие 14. Исследование механизма защиты съемных носителей с помощью СЗИ НСД (например, Страж NT)	2
	Практическое занятие 15. Исследование настройки маркировки документов с помощью СЗИ НСД (например, Страж NT)	2
Самостоятельная работа обучающихся при изучении раздела 1 - Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы. - Самостоятельное изучение законов, постановлений и других руководящих документов в области защиты информации. - Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности. - Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации		**10**
Промежуточная аттестация по МДК.03.01 в форме дифференцированного зачета		**-**
Тема 1.3. Средства защиты информации от несанкционированного доступа	**Содержание**	**40**
	1. Назначение и возможности средств защиты информации от НСД. Защита от вмешательства в процесс функционирования АС посторонних лиц	
	2. Регистрация действий пользователей. Обеспечение аутентификации абонентов	
	3. Рекомендации по выбору средств защиты информации от НСД. Распределение показателей защищенности по классам для автоматизированных систем	
	4. Требования руководящих документов ФСТЭК к средствам защиты информации	
	5. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации (например, DALLASLOCK)	
	6. Назначение, состав и возможности СЗИ (например, «Блокпост-2000» и «Блокхост-сеть»)	
	7. Назначение и особенности применения СЗИ НСД (например, «Страж NT»)	
	8. Назначение и специфика применения комплекса ЗИ (например, «Соболь»)	
	9. Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей	
	10. Назначение и функциональные возможности eToken и Рутокен. Алгоритм генерации одноразовых паролей	
	11. Формирование электронной цифровой подписи. Вычисление ключа согласования Диффи- Хеллмана	
	12. Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа	
	В том числе практических и лабораторных занятий	**16**
	Практическое занятие 16. Ввод информации в САПР СЗИ. Расчет радиуса контролируемой зоны с помощью САПР СЗИ (например, «Гроза-К»)	2

	Практическое занятие 17. Исследование защищенности с помощью САПР СЗИ. Формирование и вывод проекта протокола в САПР СЗИ (например, «Гроза-К»)	2
	Практическое занятие 18. Исследование плана тестирования при помощи СПО ЗИ. Исследование режима тестирования при помощи СПО ЗИ (например, «Ревизор-2XP»)	2
	Практическое занятие 19. Исследование содержимого текущего диска с помощью СПО ЗИ (например, «Terrier»)	4
	Лабораторное занятие 1. Исследование механизма доступа в систему с использованием СПО ЗИ и УП (например, «SecretNet»)	4
	Лабораторное занятие 2. Исследование механизма разграничения доступа с использованием СПО ЗИ и УП (например, «SecretNet»)	2
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей	**Содержание**	**32**
	1. Проблемы обеспечения безопасности в компьютерных системах и сетях. Типовая корпоративнаясеть. 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. Специализированный анализ защищенности. Обзор средств анализа защищенности	
	7. Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий	
	8. Введение в технологию обнаружения атак. Классификация систем обнаружения атак	
	В том числе практических и лабораторных занятий	**16**
	Лабораторное занятие 3. Исследование механизма контроля и регистрации с использованием СПО ЗИ и УП (например, «SecretNet»)	4
	Лабораторное занятие 4. Исследование функции отслеживания событий НСД с использованием СПО ЗИ и УП (например, «SecretNet»)	4
	Практическое занятие 20. Исследование возможности обновления клиента с использованием СПО ЗИ и УП. Исследование порядка удаления клиента с использованием СПО ЗИ и УП (например, «SecretNet»)	4
	Практическое занятие 21. Исследование проблемных ситуаций с использованием СПО ЗИ и УП (например, «SecretNet»)	4
Самостоятельная работа обучающихся при изучении раздела 1 - Дополнительное конспектирование материала по темам из рекомендуемой преподавателем литературы. - Самостоятельное изучение законов, постановлений и других руководящих документов в области защиты информации.		**4**

- Изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности. - Изучение возможностей и технических характеристик программно-аппаратных средств защиты информации. **Рекомендуемая тематика самостоятельной работы:** 1. Составление доклада по перспективе и направлению развития программно-аппаратных средств защиты информации на основе публикаций в периодической специализированной аппаратуре. 2. Практическое применение антивирусных программ для защиты информации от несанкционированного доступа. 3. Применение различных видов шифрования информации, хранящейся на ПК и выносных носителях информации с целью предотвращения несанкционированного доступа. 4. Применение различных программ для оперативного и гарантированного восстановления информации на ПК. 5. Применение программно-аппаратных средств для обеспечения разграничения доступа к защищаемой информации. 6. Разработка комплекса организационно-административной защиты от вредоносных программ. 7. Самостоятельная разработка предложений по программно-аппаратной защите информации на определенном объекте. 8. Применение подсистемы безопасности WINDOWS XP/Vista/7 для предотвращения несанкционированного доступа к защищаемой информации		
Консультации		**2**
Промежуточная аттестация по МДК.03.01 в форме экзамена		**6**
Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**138**
МДК.03.02. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи		**138**
Тема 2.1. Основы информационной безопасности	**Содержание**	**18**
	1. Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности	
	2. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере.	
	3. Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации	
	4. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности	
	В том числе лабораторных занятий	**10**
	Лабораторное занятие 1. Исследование возможностей профессионального нелинейного радиолокатора (например, NR-900EMS)	2
	Лабораторное занятие 2. Исследование возможностей многофункционального поискового прибора (например, ST 033P Пиранья)	2
	Лабораторное занятие 3. Исследование возможностей анализатора спектра (например, OSCORGreen-8)	2
	Лабораторное занятие 4. Исследование возможностей имитатора источника радиосигналов с различными видами модуляции(например, АВРОРА-3)	2
	Лабораторное занятие 5. Исследование возможностей комплекса обнаружения радиоизлучающих средств и радиомониторинга (например, КРОНА-ПРО)	2

Тема 2.2. Организационно-правовые аспекты защиты информации	**Содержание**	**14**
	1. Структура правовой защиты информации. Система документов в области защиты информации. Организационные основы защиты информации. Принципы организационной защиты информации	
	2. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации	
	3. Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере	
	В том числе лабораторных занятий	**8**
	Лабораторное занятие 6. Исследование возможностей скоростного приемника сигналов (например, СКОРПИОН-XL)	2
	Лабораторное занятие 7. Исследование принципов работы индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	2
	Лабораторное занятие 8. Исследование возможностей работы фильтров сетевых помехоподавляющих (например, ЛФС-10-1Фи ФСП-1Ф-10А)	2
	Лабораторное занятие 9. Исследование работы генератора шума для защиты от ПЭМИН (например, ЛГШ-501)	2
Тема 2.3. Комплексная система защиты информации	**Содержание**	**16**
	1. Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики 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	
	В том числе практических занятий	**6**
	Практическое занятие 1. Исследование уязвимостей и построение модели угроз объекта защиты. Разработка комплексной системы инженерно-технической защиты информации на объекте	2
	Практическое занятие 2. Исследование возможностей устройства для защиты объектов информатизации (например, СОНАТА-Р2, САЛЮТ 2000Б)	2
	Практическое занятие 3. Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок спомощью специальных устройств (например, ПРОКРУСТ-2000)	2
Тема 2.4. Инженерно-техническая защита информации	**Содержание**	**32**
	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. Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации	
	3. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД	
	4. Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению	
	5. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи	
	6. Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания	
	7. Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок	
	8. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания	
	9. Контроль слаботочных цепей. Принципы контроля линий заземления	
	10. Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации	
	11. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники	
	В том числе лабораторных занятий	**10**
	Лабораторное занятие 10. Исследование возможностей автоматизированной системы изменений сверхмалых величин. Исследование технических средств и отходящих от них линий с помощью системы измерений сверхмалых величин (например, ТАЛИС-НЧ-ЛАЙТ)	2
	Лабораторное занятие 11. Исследование возможностей системы оценки защищенности оптических линий связи. Измерение параметров ВОСП с помощью системы оценки защищенности оптических линий связи Оценка защищенности оптических линий связи с помощью системы оценки защищенности оптических линий связи (например,ЛАЗУРИТ)	2
	Лабораторное занятие 12. Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН. Оценка защищенности с использованием системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН. Измерение параметров ПЭМИН и расчет показателей защищенности технического средства (например, СИГУРД-М19)	2
	Лабораторное занятие 13. Исследование возможностей системы оценки защищенности выделенных помещений. Измерение уровня звукового давления вблизи и на удалении от источника с помощью комплекса оценки защищенности выделенных помещений (например, ШЕПОТ)	2

	Лабораторное занятие 14. Измерение уровня виброускорения в ограждающих конструкциях. Расчет и оценка защищенности помещения по акустическому каналу. Расчет и оценка защищенности помещения по виброакустическому каналу (например, с помощью комплекса ШЕПОТ)	2
Самостоятельная работа обучающихся при изучении раздела 2 - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере; - ознакомление с нормативными документами по ИБ; - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности		**2**
Промежуточная аттестация по МДК.03.02 в форме дифференцированного зачета		**-**
Тема 2.5. Криптографическая защита информации	**Содержание**	**32**
	1. Основы криптографии. Структура криптосистемы	
	2. Основные методы криптографического преобразования данных	
	3. Требования, предъявляемые к криптографическим системам. Симметричные и ассиметричные криптосистемы	
	4. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования	
	5. Криптосистемы с открытым ключом. Основы шифрования с открытым ключом	
	6. Алгоритм обмена ключами Диффи-Хеллмана	
	7. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом	
	8. Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования	
	9. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи	
	10. Понятие криптоанализа	
	В том числе практических занятий	**12**
	Практическое занятие 4. Поиск и локализация скрытых видеокамер (например, с помощью прибора ОПТИК-2)	2
	Практическое занятие 5. Исследование методов защиты сотовых телефонов от несанкционированного прослушивания (например, с помощью изделия Ладья-ИВТ)	2
	Практическое занятие 6. Исследование методов блокирования средств несанкционированного прослушивания и передачи данных различных стандартов (например, с помощью устройства КЕДР-1М)	2
	Практическое занятие 7. Поиск устройств негласного съема информации с помощью профессионального нелинейного радиолокатора (например, с помощью NR-900EMS)	2
	Практическое занятие 8. Поиск устройств негласного съема информации с помощью многофункционального поискового прибора (например, с помощью ST 033P Пиранья)	2
	Практическое занятие 9. Оценка защищенности помещения с помощью многофункционального поискового прибора (например, ST 033P Пиранья)	2
	Содержание	**18**

Тема 2.6. Аттестация и лицензирование объектов защиты	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	
	3. Программа и методика проведения аттестационных испытаний	
	4. Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации	
	5. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании	
	В том числе практических и лабораторных занятий	**8**
	Практическое занятие 10. Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля (например, РИЧ-8 / MFP-8000, ST-107, ST-165)	4
	Лабораторное занятие 15. Исследование работы генератора шума по сети электропитания и линиям заземления (например, ЛГШ-221)	2
	Практическое занятие 11. Поиск и обнаружение радиоизлучающих средств (например, с помощью комплекса КРОНА-ПРО)	2
Самостоятельная работа обучающихся при изучении раздела 2 - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере; - ознакомление с нормативными документами по ИБ; - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности; - составление доклада по перспективным направлениям развития средств комплексной защиты информации; - разработка пакета документации по инженерно-технической защите информации на объекте; - изучение возможностей инженерно-технических средств защиты информации; - изучение технических характеристик инженерно-технических средств защиты информации; - разработка предложений по инженерно-технической защите информации на определенном объекте		**6**
Промежуточная аттестация по МДК.03.02 в форме дифференцированного зачета		**-**
ПП.03.01 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**
Промежуточная аттестация по ПП.03.01 в форме дифференцированного зачета		**-**
Экзамен по модулю		**12**
Всего		**424**

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Материально-техническое обеспечение

Для реализации программы профессионального модуля предусмотрены следующие специальные помещения:

кабинет компьютерного моделирования, оснащенный в соответствии с п. 6.1.2.1 ОПОП СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи;

лаборатории информационной безопасности телекоммуникационных систем, телекоммуникационных систем, оснащенные в соответствии с п. 6.1.2.3 ОПОП СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи;

помещение для самостоятельной работы – читальный зал библиотеки, оснащенный в соответствии с п. 6.1.2.2 ОПОП СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи;

оснащенные базы практики в соответствии с п 6.1.2.5 ОПОП СПО по специальности 11.02.15 Инфокоммуникационные сети и системы связи.

4.2. Информационное обеспечение обучения

Для реализации программы библиотечный фонд образовательной организации укомплектован печатными и (или) электронными образовательными и информационными ресурсами, рекомендованными для использования в образовательном процессе.

4.2.1. Основные печатные издания

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. —5-е изд. — СПб. Питер, 2019, 2020, 2021. — 992 с. — Текст : непосредственный

4.2.2. Основные электронные издания

1. Введение в криптографическую защиту информации объектов : учебник / С. Н. Ильиных, С. Г. Алюшина, Т. И. Калинкина [и др.]. — Москва : МТУСИ, 2021. — 276 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/215231 (дата обращения: 09.02.2023). — Режим доступа: для авториз. пользователей.

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2023. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/512861 (дата обращения: 09.02.2023).

3. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/195510 (дата обращения: 09.02.2023). — Режим доступа: для авториз. пользователей.

4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364 (дата обращения: 09.02.2023).

4.2.3. Дополнительные источники

1. Лось, А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для вузов / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — Москва : Издательство Юрайт, 2023. — 473 с. — (Высшее образование).

— ISBN 978-5-534-12474-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511138 (дата обращения: 09.02.2023).

2. Мызникова, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Мызникова. — Омск : ОмГУПС, 2017. — 82 с. — ISBN 978-5-949-41160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/129192 (дата обращения: 09.02.2023). — Режим доступа: для авториз. пользователей.

4.3. Общие требования к организации образовательного процесса

Освоение программы модуля базируется на изучении дисциплин ОП.07. Основы телекоммуникаций, ОП.10. Прикладное программное обеспечение профессиональной деятельности, ОП.11. Правовое обеспечение профессиональной деятельности и профессиональных модулей ПМ.01 Техническая эксплуатация инфокоммуникационных сетей связи, ПМ.02 Техническая эксплуатация инфокоммуникационных систем.

ПП.03.01 Производственная практика (по профилю специальности) проводится концентрировано в организациях, деятельность которых соответствует профилю подготовки обучающихся.

Результаты прохождения производственной практики (по профилю специальности) по профессиональному модулю учитываются при проведении экзамена по модулю.

4.4. Кадровое обеспечение образовательного процесса

Реализация рабочей программы профессионального модуля обеспечивается педагогическими работниками образовательной организации, а также лицами, привлекаемыми к реализации образовательной программы на иных условиях, в том числе из числа руководителей и работников организаций, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии (имеющих стаж работы в данной профессиональной области не менее 3 лет).

Квалификация педагогических работников образовательной организации отвечает квалификационным требованиям, указанным в квалификационных справочниках и (или) профессиональных стандартах.

Педагогические работники, привлекаемые к реализации образовательной программы, получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки, в организациях, направление деятельности которых соответствует области профессиональной деятельности 06 Связь, информационные и коммуникационные технологии не реже 1 раза в 3 года с учетом расширения спектра профессиональных компетенций.

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

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности	- классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно; - анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный; - возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно; - мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме; - недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выявлены в полном объеме, тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно	- тестирование; - экспертное наблюдение за деятельностью обучающихся в ходе выполнения практических занятий, работ по производственной практике; - экспертная оценка деятельности обучающихся в ходе проведения практических занятий; - выполнение индивидуальных и коллективных работ (рефератов, презентаций, расчетно-графических работ, решение ситуационных задач); - дифференцированный зачет по производственной практике (по профилю специальности); - дифференцированные зачеты и экзамен по междисциплинарным курсам; - экзамен по профессиональному модулю
ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи	- для обеспечения информационной безопасности выбраны оптимальные способы; - выбор средств защиты осуществлен в соответствии с выявленными угрозами в инфокоммуникационных сетях	
ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования	- мероприятия по защите информации на предприятиях связи определены в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными; - политика безопасности сетевых элементов и логических сетей разработана в полном объеме; - расчет и установка специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей выполнены в соответствии с отраслевыми стандартами; - установка и настройка средств защиты операционных систем, инфокоммуникационных систем и сетей связи выполнена в соответствии с отраслевыми стандартами; - конфигурирование автоматизированных систем и информационно-коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами; - базы данных максимально защищены при помощи специализированных программных продуктов; - ресурсы инфокоммуникационных сетей и систем связи максимально защищены криптографическими методами	
ОК 01. Выбирать способы решения задач профессиональной	- обучающийся демонстрирует наличие умений распознавать задачу (проблему) в профессиональном или социальном контексте; анализировать и выделять её составные части;	- экспертное наблюдение за деятельностью обучающихся в ходе

деятельности применительно к различным контекстам	определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи (проблемы); составлять план действий; определять необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий	выполнения различных видов работ: - на практических занятиях; - в ходе выполнения индивидуальных и коллективных заданий (рефератов, презентаций, расчетно-графических работ, решение ситуационных задач); - в ходе выполнения работ по производственной практике (по профилю специальности); - в ходе проведения экзамена по профессиональному модулю
ОК 02. Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности	- обучающийся обладает способностью определять задачи и необходимые источники для поиска информации; планировать процесс поиска и структурировать получаемую информацию; выделять наиболее значимое в перечне информации и оценивать практическую значимость результатов поиска; оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; использовать современное программное обеспечение и различные цифровые средства для решения профессиональных задач	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях	при выполнении поставленных задач обучающийся демонстрирует способность: - определять актуальность нормативно-правовой документации в профессиональной деятельности; применять современную научную профессиональную терминологию; - определять и выстраивать траектории профессионального развития и самообразования; - использовать знания по финансовой грамотности в различных жизненных ситуациях	
ОК 04. Эффективно взаимодействовать и работать в коллективе и команде	- обучающийся демонстрирует умение организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста	- обучающийся разбирается в особенностях социального и культурного контекста, осознано применяет правила оформления документов и построения устных сообщений; грамотно излагает свои мысли и оформляет документы по профессиональной тематике на государственном языке, проявляет толерантность в рабочем коллективе	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения	- обучающийся демонстрирует знание и понимание сущности гражданско-патриотической позиции, общечеловеческих ценностей; - описывает значимость своей специальности; - применяет стандарты антикоррупционного поведения, осознает возможные последствия его нарушения	
ОК 09. Пользоваться профессиональной документацией на государственном и иностранном языках	- обучающийся понимает общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), а также тексты на базовые профессиональные темы; участвует в диалогах на знакомые общие и профессиональные темы; строит простые	

	высказывания о себе и о своей профессиональной деятельности; кратко обосновывает и объясняет свои действия (текущие и планируемые); пишет простые связные сообщения на знакомые или интересующие профессиональные темы	