МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

РОСТОВСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

РОСТОВСКОЙ ОБЛАСТИ

**«РОСТОВСКИЙ-НА-ДОНУ КОЛЛЕДЖ СВЯЗИ И ИНФОРМАТИКИ»**

**РАБОЧАЯ ПРОГРАММА**

Профессионального модуля

**ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

программы подготовки специалистов среднего звена

для специальности

**11.02.15 Инфокоммуникационные сети и системы связи**

(базовой подготовки)

г. Ростов-на-Дону

2025 г.

|  |  |
| --- | --- |
| **ОДОБРЕНО**  На заседании цикловой комиссии  «Телекоммуникаций»  Протокол № 7 от 5 февраля 2025г.  Председатель ЦК  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Л.В. Ермолина | **УТВЕРЖДАЮ:**  Зам. директора по УМР  \_\_\_\_\_\_\_\_\_\_\_\_И.В.Подцатова  «28 » февраля 2025 г. |

Рабочая программа профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 «Инфокоммуникационные сети и системы связи», утвержденного приказом Минпросвещения России от 5 августа 2022 г. № 675 (ред. от 03.07.2024 №464) «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 11.02.15 Инфокоммуникационные сети и системы связи», зарегистрированным в Минюсте России 09.09.2022 N 70031, с целью расширения основных видов профессиональной деятельности, углубления подготовки обучающихся, а так же получения дополнительных компетенций, необходимых для обеспечения конкурентоспособности выпускника в соответствии с запросами регионального рынка труда.

Организация-разработчик: Государственное бюджетное профессиональное образовательное учреждение Ростовской области «Ростовский-на-Дону колледж связи и информатики»

Разработчики:

МДК03.01 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи – Бойнар И.Н., преподаватель ГБПОУ РО «РКСИ».

МДК.03.02**.** Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи –Бойнар И.Н., преподаватель ГБПОУ РО «РКСИ»

УП.03.01 –Бойнар И.Н., преподаватель ГБПОУ РО «РКСИ»

ПП 03.01 – Бойнар И.Н., преподаватель ГБПОУ РО «РКСИ»

Рецензенты:

Копылова О.В.– преподавательГБПОУ РО «РКСИ»

Масютин А.Н. –начальник управления системных проектов Ростовского НТЦ ФГУП «НПП «Гамма»

**СОДЕРЖАНИЕ**

1. Паспорт рабочей программы частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 4
2. Результаты освоения частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 8
3. Структура и содержание частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 9
4. Условия реализации рабочей программы частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 20
5. Контроль и оценка результатов освоения частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» 24

|  |  |
| --- | --- |
|  |  |

**1 ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**1.1 Область применения рабочей программы**

Рабочая программа профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»разработана в соответствии с требованиями регионального рынка труда на основании утвержденных на цикловых комиссиях колледжа перечнем знаний, умений и навыков по специальности 11.02.15 «Инфокоммуникационные сети и системы связи» базового уровня подготовки в части освоения основного вида профессиональной деятельности (ВПД): «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие (ОК) и профессиональные компетенций (ПК).

**Владеть общими компетенциями:**

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 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 с учетом особенностей социального и культурного контекста.

ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, 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 Пользоваться профессиональной документацией на государственном и иностранном языках.

**Владеть профессиональными компетенциями:**

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 Место учебной дисциплины в структуре образовательной программы.**

**1.3 Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля**

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

**уметь:**

1. классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;
2. - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;
3. определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;
4. осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;
5. выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов;
6. выполнять тестирование систем с целью определения уровня защищенности;

определять оптимальные способы обеспечения информационной безопасности;

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

**знать:**

1. принципы построения информационно-коммуникационных сетей;
2. международные стандарты информационной безопасности для проводных и беспроводных сетей;
3. нормативно - правовые и законодательные акты в области информационной безопасности;
4. акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;
5. технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;
6. способы и методы обнаружения средств съёма информации в радиоканале;
7. классификацию угроз сетевой безопасности;
8. характерные особенности сетевых атак;
9. возможные способы несанкционированного доступа к системам связи;
10. правила проведения возможных проверок согласно нормативных документов ФСТЭК;
11. этапы определения конфиденциальности документов объекта защиты;
12. назначение, классификацию и принципы работы специализированного оборудования;
13. методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;
14. методы и средства защиты информации в телекоммуникациях от вредоносных программ;
15. технологии применения программных продуктов;
16. оборудование и сигнализацию сети абонентского доступа;
17. возможные способы, места установки и настройки программных продуктов;
18. методы и способы защиты информации, передаваемой по кабельным направляющим системам;
19. конфигурации защищаемых сетей;
20. алгоритмы работы тестовых программ;
21. средства защиты различных операционных систем и среды передачи информации;
22. способы и методы шифрования (кодирование и декодирование) информации.

Иметь навыки:

Н1 анализировать сетевую инфраструктуру;

Н2 выявлять угрозы и уязвимости в сетевой инфраструктуре;

Н3 разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

Н4 осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи;

Н5 использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи;

ПМ 03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» способствует формированию общих компетенций и профессиональных компетенций (ПК3.1, ПК 3.2, ПК 3.3, ПК 3.4, ПК 3.5) по специальности 11.02.15 «Инфокоммуникационные сети и системы связи».

|  |  |  |
| --- | --- | --- |
| **Код**  **ОК, ПК** | **Умения** | **Знания** |
| **ОК 01** | * распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; * выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; * составлять план действия; определять необходимые ресурсы; * владеть актуальными методами работы в профессиональной и смежных сферах; реализовывать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника) | * актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; * алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности |
| **ОК 02** | * определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; * оформлять результаты поиска, применять средства информационных технологий для решения профессиональных задач; * использовать современное программное обеспечение; использовать различные цифровые средства для решения профессиональных задач. | * номенклатура информационных источников, применяемых в профессиональной деятельности; * приемы структурирования информации; * формат оформления результатов поиска информации, современные средства и устройства информатизации; * порядок их применения и программное обеспечение в профессиональной деятельности, в том числе с использованием цифровых средств. |
| **ОК 03** | * определять актуальность нормативно-правовой документации в профессиональной деятельности; * применять современную научную профессиональную терминологию; определять и выстраивать траектории профессионального развития и самообразования; * выявлять достоинства и недостатки коммерческой идеи; * презентовать идеи открытия собственного дела в профессиональной деятельности; * оформлять бизнес-план; рассчитывать размеры выплат по процентным ставкам кредитования; определять инвестиционную привлекательность коммерческих идей в рамках профессиональной деятельности; * презентовать бизнес-идею; * определять источники финансирования | * содержание актуальной нормативно-правовой документации; * современная научная и профессиональная терминология; * возможные траектории профессионального развития и самообразования; основы предпринимательской деятельности; * основы финансовой грамотности; правила разработки бизнес-планов; * порядок выстраивания презентации; * кредитные банковские продукты |
| **ОК 04** | * организовывать работу коллектива и команды; * взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности | * психологические основы деятельности коллектива, психологические особенности личности; * основы проектной деятельности |
| **ОК 05** | * грамотно излагать свои мысли и оформлять документы по профессиональной тематике на государственном языке, проявлять толерантность в рабочем коллективе | * особенности социального и культурного контекста; * правила оформления документов и построения устных сообщений |
| **ОК 06** | * описывать значимость своей специальности; * применять стандарты антикоррупционного поведения | * сущность гражданско-патриотической позиции, общечеловеческих ценностей; * значимость профессиональной деятельности по специальности; * стандарты антикоррупционного поведения и последствия его нарушения |
| **ОК 07** | * соблюдать нормы экологической безопасности; * определять направления ресурсосбережения в рамках профессиональной деятельности по специальности осуществлять работу с соблюдением принципов бережливого производства; * организовывать профессиональную деятельность с учетом знаний об изменении климатических условий региона. | * правила экологической безопасности при ведении профессиональной деятельности; * основные ресурсы, задействованные в профессиональной деятельности; * пути обеспечения ресурсосбережения; принципы бережливого производства; * основные направления изменения климатических условий региона. |
| **ОК 08** | * использовать физкультурно-оздоровительную деятельность для укрепления здоровья, достижения жизненных и профессиональных целей; * применять рациональные приемы двигательных функций в профессиональной деятельности; * пользоваться средствами профилактики перенапряжения, характерными для данной специальности | * роль физической культуры в общекультурном, профессиональном и социальном развитии человека; * основы здорового образа жизни; условия профессиональной деятельности и зоны риска физического здоровья для специальности; * средства профилактики перенапряжения |
| **ОК 09** | * понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; * участвовать в диалогах на знакомые общие и профессиональные темы; * строить простые высказывания о себе и о своей профессиональной деятельности; * кратко обосновывать и объяснять свои действия (текущие и планируемые); * писать простые связные сообщения на знакомые или интересующие профессиональные темы | * правила построения простых и сложных предложений на профессиональные темы; * основные общеупотребительные глаголы (бытовая и профессиональная лексика); * лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; * особенности произношения; правила чтения текстов профессиональной направленности |
| **ПК 3.1.** | * 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 спеиализированных программных продукты * выполнять тестирование систем с целью определения уровня защищенности. | * - 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 пред-приятий 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. |
| **ПК 3.2.** | * определять оптимальные способы обеспечения информационной безопасности; * проводить выбор средств защиты в соответствии с выявленными угрозами в инфо-коммуникационных сетях | * 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 |
| ПК 3.3. | * 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. | * методы и способы защиты информации, передаваемой по кабельным направляющим системам; * конфигурации защищаемых сетей; * алгоритмы работы тестовых программ; * средства защиты различных операционных систем и среды передачи информации; * способы и методы шифрования (кодирование и декодирование) информации. |

**1.3 Практическая подготовка при реализации учебных дисциплин путем проведения практически занятий**

Образовательная деятельность в форме практической подготовки: реализуется при проведении всех практических занятий ПМ.03, всех видов практики и иных видов учебной деятельности.

|  |  |  |
| --- | --- | --- |
| **Количество часов по учебному плану на практические занятия** | **в том числе, практическая подготовка** | **Наименование тем практических работ в форме практической подготовки с учетом специфики осваиваемой специальности** |
| **78** | **78** | **МДК 03.01 Эксплуатация объектов сетевой инфраструктуры**  Тема 1.1 Основы безопасности информационных технологий  Практическое занятие№1 Регистрация пользователей c помощью СПО ЗИ  Практическое занятие№2 Установка прав доступа c помощью СПО ЗИ  Практическое занятие№3 Настройка аудита с помощью СПО ЗИ  Практическое занятие№4 Настройка параметров политики безопасности операционной системы  Практическое занятие №5 Архивация и восстановление данных  Практическое занятие№6 Предотвращение и исправление ошибок жесткого диска  Практическое занятие№7 Сканирование логических дисков c помощью СПО ЗИ  Практическое занятие№8 Программа поиска и гарантированного уничтожения информации на дисках  Тема 1.3 Средства защиты информации от несанкционированного доступа  Практическое занятие№9 Установка и снятие СЗИ с помощью программы СЗИ НСД  Практическое занятие№10 Исследование учета пользователей и контроля устройств с помощью СЗИ НСД  Практическое занятие№11 Исследование избирательного управления с помощью СЗИ НСД  Практическое занятие№12. Исследование механизма защиты съемных носителей с помощью СЗИ НСД  Практическое занятие№13. Исследование настройки маркировки документов с помощью СЗИ НСД  Практическое занятие№14. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации  Практическое занятие№15. Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей  Практическое занятие№16. Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности  Тема 1.4 Обеспечение безопасности компьютерных систем и сетей  Практическое занятие№17Исследование работы межсетевого экрана  Практическое занятие№18. Локальные и сетевые системы обнаружения атак.  Практическое занятие№19 Работа в программе Wireshark  Практическое занятие№20. Анализ протоколов Ethernet и ARP.  Практическое занятие№21. Аудит системы безопасности |
| **72** | **72** | **МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**  Тема 1.1Основы информационной безопасности  Практическое занятие№1. Исследование уязвимостей и построение модели угроз объекта защиты.  Практическое занятие№2. Разработка модели нарушителя.  Практическое занятие№3.Подготовка технического паспорта объекта защиты  Тема2.2 Комплексная система защиты информации  Практическое занятие№4Методы аутентификации, использующие пароли. Настройка параметров аутентификации  Практическое занятие№5 Назначение прав пользователей при произвольном управлении доступом в ОС  Практическое занятие№6 Настройка защитных механизмов ОС  Практическое занятие№7 Установка и настройка межсетевого экрана  Тема 2.3 Инженерно-техническая защита информации  Практическое занятие№ 8 Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН  Практическое занятие№ 9 Исследование работы генератора шума для защиты от ПЭМИН  Практическое занятие№10 Исследование принципов работы индикаторов поля  Практическое занятие№11 Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств  Практическое занятие№12 Исследование возможностей профессионального нелинейного радиолокатора  Практическое занятие№ 13 Исследование возможностей многофункционального поискового прибора  Практическое занятие№ 14 Установка и настройка программных средств защиты телекоммуникационных систем и сетей электросвязи  Практическое занятие№15 Установка и настройка датчиков контроля вскрытия линейно-кабельных сооружений и устройств  Практическое занятие№16 Установка и настройка датчиков тревожной сигнализации  Практическое занятие№17 Поиск и локализация скрытых видеокамер  Практическое занятие№18 Разработка технического задания на создание защиты информационной системы  Тема 2.4 Криптографическая защита информации  Практическое занятие№19 Шифрование методами перестановки и простой замены  Практическое занятие№ 20 Шифрующая файловая система EFS и управление сертификатами в ОС  Практическое занятие№ 21 Построение виртуальных сетей  Тема 2.5 Аттестация и лицензирование объектов защиты  Практическое занятие№ 22 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации.  Практическое занятие№ 23 Анализ информационных ресурсов, циркулирующих в организации.  Практическое занятие№ 24 Анализ программно-технических средств, используемых в организации.  Практическое занятие№ 25 Анализ защищаемого помещения и каналов утечки информации.  Практическое занятие№ 26 Составление комплекта документации для лицензирования работ и услуг в области защиты информации (ФСТЭК). |

**2.РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Результатом освоения профессионального модуля **ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»** является овладение обучающимися видом профессиональной деятельности (ВПД), в том числе профессиональными компетенциями (ПК), общими компетенциями (ОК)

|  |  |
| --- | --- |
| **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 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 с учетом особенностей социального и культурного контекста. |
| ОК 06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, 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 | Пользоваться профессиональной документацией на государственном и иностранном языках. |

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 |

**3.СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**

**3.1. Объем учебной дисциплины и виды учебной работы**

|  |  |
| --- | --- |
| **Вид учебной работы** | ***Объем часов*** |
| **Максимальная учебная нагрузка (всего)** | *294* |
| **Обязательная аудиторная учебная нагрузка (всего)** | *210* |
| в том числе: |  |
| теоретическое обучение | *60* |
| практические занятия (*если предусмотрено)* | *150* |
| **Самостоятельная работа обучающегося (всего)** |  |
| в том числе |  |
| подготовка к аудиторным занятиям |  |
| ***Учебная практика*** | *36* |
| ***Производственная практика (по профилю специальности)*** | *36* |
| ***Промежуточная аттестация – квалификационный экзамен*** | *12* |

**3.Сруктура и содержание профессионального модуля.**

**3.1 Тематический план профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Коды профессиона  льных общих компетенций | Наименования разделов профессионального модуля | Суммарный объем  нагрузки, час. |  | Объем профессионального модуля, час. | | | | | Самостоят ельная  работа |
|  | *Обучение по МДК* | | | *Практики* | |
| Всего | *В том числе* | | |
| Лабораторных и практических занятий | | Курсовых работ  (проектов) | Учебная | Производственная |
| ПК 3.1-3.3 ОК 01-09 | **МДК 03.01**Применение программно- аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи | 108 | 108 | 78 | | - | 36 | - | - |
| ПК 3.1-3.3 ОК 01-09 | **МДК 03.02**Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи | 102 | 102 | 72 | |  | 36 | - |
| ПК 3.1-3.3 ОК 01-09 | Учебная практика *(по профилю специальности, часов(концентрированная) практика)* | 36 |  |  | |  | 36 | - |  |
| ПК 3.1-3.3 ОК 01-09 | Производственная практика *(по профилю специальности), часов (концентрированная) практика)* | 36 |  |  | | | | 36 |  |
| Промежуточная аттестация (экзамен) | 12 |  |  | | | |  |  |
|  | **Всего:** | **294** | **210** |  | **150** |  | **36** | **36** | **-** |

**3.2 Содержание частично вариативного профессионального модуля ПМ.03 «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи»**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Наименование разделов и тем профессионального модуля (ПМ), меж-дисциплинарных курсов (МДК)** | **Содержание учебного материала практические занятия, внеаудиторная (самостоятельная) учебная работа обучающихся, курсовая работа (проект)** | | **Объем часов** | **Формируемые**  **ОК, ПК** |
| **1** | **2** | | **3** |  |
| **МДК 03.01. Применение программно- аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи** | | |  |  |
| **Тема 1.1.**Основы безопасности информационных технологий | **Содержание** | | **12** |  |
| 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 | ПК-3.1-3.3  ОК-1-9 |
| 2. **Основные понятия в области безопасности информационных технологий.** Информация и информационные отношения. Субъекты информационных отношений, их безопасность. | | 2 |
| 3. **Угрозы безопасности информационных технологий**. Уязвимость основных структурно-функциональных элементов распределенных автоматизированных систем. Классификация угроз безопасности. | | 2 |
| 4. **Принципы обеспечения безопасности информационных технологий**. Виды мер противодействия угрозам безопасности. Достоинства и недостатки различных видов мер защиты. Принципы построения системы обеспечения безопасности информации в автоматизированной системе. | | 2 |
| 5. **Защищаемая информация.** Правовые основы обеспечения безопасности информационных технологий. Персональные данные. Коммерческая тайна. Информация в ключевых системах информационной инфраструктуры. Государственная система защита информации. Организация защиты информации в системах и средствах информатизации и связи. Контроль состояния защиты информации. | | 2 |
| 6. **Идентификация и аутентификация пользователей.** Основные защитные механизмы, реализуемые в рамках различных мер и средств защиты. Разграничение доступа зарегистрированных пользователей к ресурсам автоматизированной системы. Регистрация и оперативное оповещение о событиях безопасности. | | 2 |  |
|  | **Практические занятия** | | **28** |  |
| 1. Регистрация пользователей c помощью СПО ЗИ | | 6 | ПК-3.1-3.3  ОК-1-9 |
| 2. Установка прав доступа c помощью СПО ЗИ | | 4 |
| 2. Настройка аудита с помощью СПО ЗИ | | 2 |
| 3. Настройка параметров политики безопасности операционной системы | | 4 |
| 4. Архивация и восстановление данных | | 2 |
| 5. Предотвращение и исправление ошибок жесткого диска | | 4 |
| 6. Сканирование логических дисков c помощью СПО ЗИ | | 2 |
| 7. Программа поиска и гарантированного уничтожения информации на дисках | | 2 |
| **Тема 1.2.**Обеспечение безопасности информационных технологий | **Содержание** | | **12** |  |
| **1. Понятие технологии обеспечения безопасности информации.** Влияние на безопасность со стороны руководства организаций. Институт ответственных за обеспечение безопасности ИТ. | | 2 | ПК-3.1-3.3  ОК-1-9 |
| **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. Документы, регламентирующие правила парольной и антивирусной защиты. Инструкция по организации парольной защиты. Инструкция по организации антивирусной защиты. Документы, регламентирующие порядок допуска к работе и изменения полномочий пользователей. Регламентация допуска сотрудников. Правила именования пользователей. Процедур авторизации сотрудников. | | 4 |
| **3. Порядок изменения конфигурации программно-аппаратных средств**. Обеспечение и контроль физической целостности и неизменности конфигурации аппаратно-программных средств автоматизированной системы. Экстренная модификация. | | 2 |
| **4. Определение требований к защите и категорирование ресурсов.** Определение градаций важности и соответствующих уровней обеспечения защиты ресурсов. Категорирование защищаемых ресурсов. Проведение информационных обследований и документирование защищаемых ресурсов. | | 2 |
| **5. Основные задачи подразделений обеспечения безопасности ИТ.** Организационная структура подразделения безопасности. Организационно-правовой статус службы обеспечения безопасности информации. | | 2 |
| **Тема 1.3.**Средства защиты информации от несанкционированного доступа | | **Содержание** | **4** |  |
| **1. Назначение и возможности средств защиты информации от НСД**. Защита от вмешательства в процесс функционирования АС посторонних лиц. Регистрация действий пользователей. Обеспечение аутентификации абонентов. | 2 | ПК-3.1-3.3  ОК-1-9 |
| **2. Рекомендации по выбору средств защиты информации от НСД**. Распределение показателей защищенности по классам для автоматизированных систем. Требования руководящих документов ФСТЭК к средствам защиты информации. | 2 |
| **Практические занятия** | **28** |  |
| 8. Установка и снятие СЗИ с помощью программы СЗИ НСД | 4 | ПК-3.1-3.3  ОК-1-9 |
| 9. Исследование учета пользователей и контроля устройств с помощью СЗИ НСД | 4 |
| 10. Исследование избирательного управления с помощью СЗИ НСД | 2 |
| 11. Исследование механизма защиты съемных носителей с помощью СЗИ НСД | 2 |
| 12. Исследование настройки маркировки документов с помощью СЗИ НСД | 2 |
| 13. Назначение и возможности аппаратно-программного комплекса СЗИ и аутентификации | 4 |
| 14. Устройства аутентификации на базе смарт-карт и USB-токенов. Реализация схем аутентификации. Программные средства, реализующие инфраструктуру открытых ключей | 4 |
| 15. Особенности разграничения доступа к ресурсам системы. Избирательное разграничение доступа. Полномочное разграничение доступа. Регистрация событий, имеющих отношение к безопасности | 6 |
| **Тема 1.4.**Обеспечение безопасности компьютерных систем и сетей | | **Содержание** | **6** |  |
| **1. Проблемы обеспечения безопасности в компьютерных системах и сетях**. Типовая корпоративная сеть. Уязвимости и их классификация. | 2 | ПК-3.1-3.3  ОК-1-9 |
| **2. Назначение, возможности и защитные механизмы межсетевых экранов.** Угрозы, связанные с периметром сети. Типы межсетевых экранов. Сертификация межсетевых экранов. | 2 |
| 3. **Обнаружение и устранение уязвимостей**. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Специализированный анализ защищенности. Обзор средств анализа защищенности. Мониторинг событий безопасности. Инфраструктура управления журналами событий. Категории журналов событий. Введение в технологию обнаружения атак. Классификация систем обнаружения атак. | 2 |
| **Практические занятия** | **24** |
| 16. Исследование работы межсетевого экрана | 6 |
| 17. Локальные и сетевые системы обнаружения атак. | 4 |  |
|  | | 18. Работа в программе Wireshark | 4 |
|  | | 19. Анализ протоколов Ethernet и ARP. | 2 |
|  | | 20. Аудит системы безопасности | 4 |
| 7 семестр Всего 108 часов из них 30 теории, 78 практики  Промежуточная аттестация в форме другой формы контроля | | | | |

|  |  |  |
| --- | --- | --- |
| **Учебная практика УП.03.01**  **ВИДЫ РАБОТ:**  Использование программно-аппаратных средств защиты информации в телекоммуникационных системах и сетях связи.  Применение систем анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдача рекомендаций по их устранению.  Обеспечение безопасного администрирования телекоммуникационных систем и информационно-коммуникационных сетей связи. | 36 | ПК-3.1-3.3  ОК-1-9 |
| Тема 1 Установка и настройка средств технической защиты информации | 12 |
| Тема 2 Анализ защищенности ТКС | 6 |
| Тема 3 Защита информации в корпоративной сети | 16 |
| Промежуточная аттестация в форме зачета | 2 |

|  |  |  |  |
| --- | --- | --- | --- |
| **1** | **2** | **3** | **4** |
| **МДК 03.02 Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи** | |  |  |
| **Раздел 1Сущность и задачи комплексной системы защиты информации** | |  |  |
| **Тема 1.1** Основы информационной безопасности | **Содержание** | **16** | ПК-3.1-3.3  ОК-1-9 |
| 1.**Основные понятия информационной безопасности.** Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности. | 2 |
| 2. **Основные составляющие национальных интересов Российской Федерации в информационной сфере**. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности. | 2 |
| 3. **Виды и источники угроз информационной безопасности Российской Федерации.** Доктрина информационной безопасности Российской Федерации. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. | 2 |
| **Практические занятия** | **10** |
| 1. Исследование уязвимостей и построение модели угроз объекта защиты. | 4 |
| 2. Разработка модели нарушителя. | 2 |
| 3.Подготовка технического паспорта объекта защиты | 4 |
| **Раздел 2 Инженерно-технические средства защиты информации** | |  |  |
| **Тема 2.1** Организационно-правовые аспекты защиты информации | **Содержание** | **4** | ПК-3.1-3.3  ОК-1-9 |
| 1. **Структура правовой защиты информации**. Система документов в области защиты информации. Организационные основы защиты информации. Принципы организационной защиты информации. 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. | 2 |
|  | 2. **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. | 2 |  |
| **Тема2.2** Комплексная система защиты информации | **Содержание** | **16** | ПК-3.1-3.3  ОК-1-9 |
| 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 |
| 2. **Система физической защиты**. Обобщенная структурная схема охраны объекта. Посты охраны. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение. | 2 |
| **Практические занятия** | **12** |
| 4 Методы аутентификации, использующие пароли. Настройка параметров аутентификации | 2 |
| 5 Назначение прав пользователей при произвольном управлении доступом в ОС | 2 |
| 6 Настройка защитных механизмов ОС | 4 |
| 7 Установка и настройка межсетевого экрана | 4 |
| **Тема 2.3** Инженерно-техническая защита информации | **Содержание** | **34** | ПК-3.1-3.3  ОК-1-9 |
| 1.**Основы инженерно-технической защиты информации**. Подразделения технической защиты информации и их основные задачи. Механические системы защиты.  Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. | 2 |
| 2. **Защита информации от утечки по техническим каналам передачи информации.**Пассивное противодействие НСД. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи. | 2 |
| 3. **Демаскирующие признаки закладных устройств**. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок. | 2 |
| 4. **Контроль линий связи, отходящих от технических средств**. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. Контроль слаботочных цепей. Принципы контроля линий заземления. | 2 |
| 5. **Средства нелинейной радиолокации**. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники. | 2 |
|  | **Практические занятия** | **24** |  |
| 8 Исследование возможностей системы оценки защищенности технических средств от утечки информации по каналу ПЭМИН | 2 |
| 9 Исследование работы генератора шума для защиты от ПЭМИН | 2 |
| 10 Исследование принципов работы индикаторов поля | 2 |
| 11 Методы защиты телефонных переговоров от прослушивания и обнаружения телефонных закладок с помощью специальных устройств | 2 |
| 12 Исследование возможностей профессионального нелинейного радиолокатора | 2 |
| 13 Исследование возможностей многофункционального поискового прибора | 2 |
| 14 Установка и настройка программных средств защиты телекоммуникационных систем и сетей электросвязи | 2 |
| 15 Установка и настройка датчиков контроля вскрытия линейно-кабельных сооружений и устройств | 2 |
| 16 Установка и настройка датчиков тревожной сигнализации | 2 |
| 17 Поиск и локализация скрытых видеокамер | 2 |
| 18 Разработка технического задания на создание защиты информационной системы | 4 |
| **Тема 2.4** Криптографическая защита информации | **Содержание** | **18** | ПК-3.1-3.3  ОК-1-9 |
| 1.**Основы криптографии.** Структура криптосистемы. Основные методы криптографического преобразования данных.Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования.Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. | 2 |
| 2. **Электронная подпись.** Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода *CRC*. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа. | 2 |
| **Практические занятия** | **14** |  |
| 19 Шифрование методами перестановки и простой замены | 2 |
| 20 Шифрующая файловая система EFS и управление сертификатами в ОС | 4 |
| 21 Построение виртуальных сетей | 8 |  |
| **Тема 2.5** Аттестация и лицензирование объектов защиты | **Содержание** | **14** |  |
| 1. **Порядок проведения аттестации объектов информатизации**. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний. Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании. | 2 | ПК-3.1-3.3  ОК-1-9 |
| **Практические занятия** | **12** |
| 22 Изучение положения по аттестации объектов информатизации по требованиям безопасности информации. | 2 |
| 23 Анализ информационных ресурсов, циркулирующих в организации. | 2 |
| 24 Анализ программно-технических средств, используемых в организации. | 2 |
| 25 Анализ защищаемого помещения и каналов утечки информации. | 2 |
| 26 Составление комплекта документации для лицензирования работ и услуг в области защиты информации (ФСТЭК). | 4 |
| **Итого** | | **102** |  |
| **8 семестр** | **Всего 102 часа из них 30 теории, 72 практических занятий** |  |  |
| Промежуточная аттестация в форме другой формы контроля | |  |  |

**Производственная практика ПП 03 (по профилю специальности)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Код  **ПК** | **Код и наименования профессиональных модулей** | **Количество**  **часов по ПМ** | **Виды работ** | **Наименования тем производственной практики** | **Кол-во**  **часов**  **по**  **темам** |
| ПК-3.1-3.3 | ПМ .03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи | 36 | 1. Участие в создании комплексной системы защиты на предприятии.  2. Применение программно-аппаратных средств защиты информации на предприятии.  3. Осуществление текущего администрирования для защиты инфокоммуникационных сетей и систем связи.  4. Проведение анализа сетевой инфраструктуры, мониторинга сети.  5. Выявление угроз и уязвимости в сетевой инфраструктуре.  6. Применение специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.  7. Применение инженерно-технических средств защиты информации на предприятии. | Тема 1 Знакомство с предприятием: инструктаж по охране труда и технике безопасности; экскурсия по предприятию; изучение правил внутреннего распорядка, режима работы сотрудников и практикантов. | 4 |
| Тема 2 Изучение структуры предприятия. Знакомство с ролью данного предприятия связи в структуре отрасли; изучение организационной структуры предприятия; изучение перечня предоставляемых услуг; изучение схемы организации связей. | 2 |
| Тема 3 Обслуживание технических средств защиты информации от несанкционированного доступа. | 6 |
| Тема 4Участие в работах по диагностике и мониторингу систем безопасности в компьютерных системах и сетях. | 6 |
| Тема 5 Изучение инструкций, документации по обеспечение безопасности информационных технологий, компьютерных систем и сетей | 6 |
| Тема 6 Самостоятельная работа на закрепленном рабочем месте. | 8 |
| Тема 7 Обобщение материала, оформление дневника, отчета, сдача зачета. | 4 |

**4 УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**4.1Требования к минимальному материально-техническому обеспечению.**

Реализация рабочей программы профессионального модуля требует наличия:

* учебных кабинетов, лабораторий, мастерских:
* Кабинет «Компьютерного моделирования»,
* лаборатории «Информационной безопасности телекоммуникационных систем»,
* «Телекоммуникационных систем»;

⮚ оборудования учебных кабинетов, лабораторий:

* автоматизированные рабочие места по количеству обучающихся;
* автоматизированное рабочее место преподавателя;
* специализированная мебель;
* комплект нормативных документов;
* комплект учебно-методической документации.
* технических средств обучения и средств информационных технологий, включая программное обеспечение:
* проектор;
* сканер;
* принтер;
* компьютеры в комплекте (системный блок, монитор, клавиатура, манипулятор «мышь») или ноутбуки (моноблоки),
* локальная сеть с выходом в Интернет,
* комплект проекционного оборудования (интерактивная доска в комплекте с проектором или мультимедийный проектор с экраном)
* программно-аппаратный межсетевой экран (комплекс сетевой защиты)
* комплекс антивирусного программного обеспечения,
* комплекс программного обеспечения шифрования и дешифрования данных с использованием различных систем шифрования,
* устройства защиты слаботочных систем коммуникаций (телефонная линия, радиотрансляция)

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

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

Рекомендуемая литература:

Основные источники:

**МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях электросвязи**

1. Родичев, Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие/ Ю.А. Родичев – СПб: Питер, 2019. – 304 с.: ил. – ISBN 978-5-4461-1275-3.
2. Нестеров, С.А. Основы информационной безопасности. Учебник для вузов/ С.А. Нестеров – М.: Лань, 2021. – 324 с.: ил. – ISBN 978-5-8114-6738-9.
3. Партыка Т.Л. Вычислительная техника: учеб. пособие / Т.Л. Партыка, И.И. Попов. — 3-е изд., перераб. и доп. — М.: ФОРУМ: ИНФРА-М, 2017. — 445 с.: ил. — (Среднее профессиональное образование). ISBN: 978-5-91134-646-1.
4. Назаров, А.В. Эксплуатация объектов сетевой инфраструктуры: учебник/ А. В.Назаров. - М.: Академия, 2018.- 368с. ISBN 978-5-44680347-7.
5. Технологии защиты информации в компьютерных сетях : учебное пособие / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.
6. Шива Парарасрам, Алекс Замм, Kali Linux Тестирование на проникновение и безопасность. Изд. Питер, 2020, 441 стр.
7. А.П. Душкин. Программно-аппаратные средства обеспечения информационной безопасности. Изд.: Москва Горячая линия- Телеком, 2020, 242 cтр.
8. А.О. Чефранова, Технология построения VPN VipNet: курс лекций. Тзд.: Москва Горячая линия – Телекос, 2022. 334 стр.
9. 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, 2021. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2.
10. Внуков, А. А.  Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2022. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8.
11. Букатов Александр Алексеевич, Гуда Сергей Александрович. Компьютерные сети. Расширенный начальный курс. Спб. : Питер, 2019.
12. Олифер, В.Г. Компьютерные сети: Принципы, технологии, протоколы : Учеб. пособие для вузов / В. Г. Олифер, Н.А. Олифер. Спб. : Питер, 2019.
13. Таненбаум Эндрю, Бос Х. Современные операционные системы. Изд. – Спб.: Питер, 2020, 1120 стр.
14. Скрипник Д. А. Общие вопросы технической защиты информации: учебное пособие / Скрипник Д. А. –М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.
15. Гребешков, А. Ю. Аппаратные средства телекоммуникационных систем: учебное пособие / А. Ю. Гребешков. - Самара: Поволжский государственный университет телекоммуникаций и информатики, 2017. - 295 c.
16. Никифоров, С. Н. Защита информации. Защита от внешних вторжений : учебное пособие / С. Н. Никифоров. - Санкт-Петербург : Санкт-Петербургский государственный архитектурно-строительный университет, ЭБС АСВ, 2017. - 84 c.

**МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи**

1. Сорокин, А. С. Основы построения защищенных инфокоммуникационных систем : учебно-методическое пособие / А. С. Сорокин. - Москва : Московский технический университет связи и информатики, 2018. - 49 c.
2. Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. - Саратов : Ай Пи Эр Медиа, 2019. - 227 c.
3. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. - 2-е изд. - Саратов : Профобразование, 2019. - 702 c.
4. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 c.
5. Скрипник, Д. А. Общие вопросы технической защиты информации: учебное пособие / Д. А. Скрипник. - 3-е изд. - Москва, Саратов : ИнтернетУниверситет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2019. - 424 c.

**Дополнительные источники**

Научно-технические и реферативные журналы:

1. Электросвязь

2. Вестник связи

3. Сети и системы связи

4. Мобильные системы

5. Цифровая обработка сигналов

6. Сводный реферативный журнал "Связь".

**Интернет-ресурсы:**

1. Информационно-справочная система по документам в области технической защиты информации [www.fstec.ru](http://www.fstec.ru)
2. Информационный портал по безопасности [www.SecurityLab.ru](http://www.securitylab.ru).
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Российский биометрический портал [www.biometrics.ru](http://www.biometrics.ru)
5. Сайт журнала Информационная безопасность http://www.itsec.ru –
6. Сайт Научной электронной библиотеки [www.elibrary.ru](http://www.elibrary.ru)
7. Справочно-правовая система «Гарант» » [www.garant.ru](http://www.garant.ru)
8. Справочно-правовая система «Консультант Плюс» [www.consultant.ru](http://www.consultant.ru)
9. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) [www.fstec.ru](http://www.fstec.ru)
10. Федеральный портал «Информационно-коммуникационные технологии в образовании» htpp\\[:www.ict.edu.ru](http://www.ict.edu.ru/)

Федеральный портал «Российское образование [www.edu.ru](http://www.edu.ru/)

* 1. **Общие требования к организации образовательного процесса**

Перед изучением профессионального модуля обучающиеся изучают следующие учебные дисциплины:

* «Основы электронной и вычислительной техники»,
* «Основы телекоммуникаций».
* «Электрорадиоизмерения»,
* Операционные системы».

**4.4Кадровое обеспечение образовательного процесса**

Образование педагогических работников соответствует профилю преподаваемого профессионального модуля, а повышение квалификации - требованиям ФГОС СПО.

1. Квалификация педагогических (инженерно-педагогических) кадров, обеспечивающих обучение по междисциплинарным курсам:

МДК.03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи – Бойнар И.Н. -  преподаватель высшей квалификационной категории;

МДК.03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи – Бойнар И.Н. -  преподаватель высшей квалификационной категории;

2. Квалификация педагогических (инженерно-педагогических) кадров, осуществляющих руководство практикой:

УП03.01 «Защита информации» - Бойнар И.Н. -  преподаватель высшей квалификационной категории;

ПП03.01 Производственная практика (по профилю специальности) – Бойнар И.Н. -  преподаватель высшей квалификационной категории.

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

Организация и порядок текущего контроля и промежуточной аттестации регулируются локальным «Положением о текущем контроле и промежуточной аттестации студентов ГБПОУ РО «РКСИ»

|  |  |  |  |
| --- | --- | --- | --- |
| **Результаты обучения**  **(освоенные профессиональные компетенции *и профессиональные компетенции*)**   |  | | --- | |  | | **Основные показатели оценки результатов обучения** | **Формы, методы  контроля и оценки  результатов обучения** |
| **ПК 3.1** Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности. | Знает классифицирование угроз информационной безопасности в инфокоммуникационных системах и сетях связи осуществляется верно;  Умеет проводить анализ угроз и уязвимостей сетевой безопасности *IP*-сетей, беспроводных сетей, корпоративных сетей обоснованный и полный;  Знает возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи определены верно;  Умеет проводить мероприятия по проведению аттестационных работ и выявлению каналов утечки осуществляются в полном объеме;  Знает недостатки систем защиты в системах и сетях связи с использованием специализированных программных  продукты выявлены в полном объеме;  Умеет проводить тестирование систем с целью определения уровня защищенности выполнено, уровень защищенности определен верно. | устный опрос,  тестирование,  практическая проверка, собеседование,  зачет по учебной практике,  зачет по производственной практике,  Квалификационный экзамен |
| **ПК 3.2** Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. | Умеет для обеспечения информационной безопасности выбирать оптимальные способы;  выбирает средства защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях. | устный опрос,  тестирование,  практическая проверка, собеседование,  зачет по учебной практике,  зачет по производственной практике,  Квалификационный экзамен |
| **ПК 3.3** Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. | Определяетмероприятия по защите информации на предприятиях связи в полном объеме, их организация, способы и методы реализации являются оптимальными и достаточными;  Разрабатываетполитику безопасности сетевых элементов и логических сетей в полном объеме;  Выполняет расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей в соответствии с отраслевыми стандартами;  Умеет выполнять установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи в соответствии с отраслевыми стандартами;  Осуществляет конфигурирование автоматизированных систем и информационно коммуникационных сетей осуществлено в соответствии с политикой информационной безопасности и отраслевыми стандартами;  Выполняет защиту базы данных максимально при помощи специализированных программных продуктов;  Умеет выполнить защиту ресурсов инфокоммуникационных сетей и систем связи максимально криптографическими методами | устный опрос,  тестирование,  практическая проверка, собеседование,  зачет по учебной практике,  зачет по производственной практике,  Квалификационный экзамен |
| ОК 01 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам | * обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; * адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач. | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 02 Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 03 Планировать и реализовывать собственное профессиональное личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях | - демонстрация ответственности за принятые решения  - обоснованность самоанализа и коррекция результатов собственной работы; | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 04 Эффективно взаимодействовать и работать в коллективе и команде | - конструктивное взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;  - обоснованность анализа работы членов команды (подчиненных) | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 05 Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста | * грамотность устной и письменной речи; * ясность формулирования и изложения мыслей. | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 06 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения | соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, демонстрация соблюдения стандартов антикоррупционного поведения | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 07 Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;  - знание и использование ресурсосберегающих технологий в области телекоммуникаций | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 08 Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |
| ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. | - устный опрос;  - практическая проверка;  - собеседование;  - зачет по учебной практике,  -зачет по производственной практике,  - квалификационный экзамен |

Лист изменений

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

Дополнений и изменений к рабочей программе ПМ на 2026/2027 учебный год

Дополнения и изменения в рабочей программе ПМ обсуждены на заседании ЦК Телекоммуникаций

Протокол № \_\_\_\_\_\_ от «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 202\_\_г.

Председатель ЦК: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_