# АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
# ПМ.03 Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи

## 1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций

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

1.1.2. Перечень профессиональных компетенций

| Код | Наименование видов деятельности и профессиональных компетенций |
|---|---|
| **ВД 1** | 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. |

1.1.3. В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| Иметь практический опыт: | - выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;<br>- разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; |

| | |
|---|---|
| | - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. |
| Уметь: | классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;<br>проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;<br>определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;<br>осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;<br>выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты<br>выполнять тестирование систем с целью определения уровня защищенности;<br>определять оптимальные способы обеспечения информационной безопасности;<br>проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;<br>проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;<br>разрабатывать политику безопасности сетевых элементов и логических сетей;<br>выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;<br>производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;<br>конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;<br>защищать базы данных при помощи специализированных программных продуктов;<br>защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами. |
| Знать: | принципы построения информационно-коммуникационных сетей;<br>международные стандарты информационной безопасности для проводных и беспроводных сетей;<br>нормативно - правовые и законодательные акты в области информационной безопасности;<br>акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;<br>технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;<br>способы и методы обнаружения средств съёма информации в радиоканале;<br>классификацию угроз сетевой безопасности;<br>характерные особенности сетевых атак;<br>возможные способы несанкционированного доступа к системам связи;<br>правила проведения возможных проверок согласно нормативных документов ФСТЭК;<br>этапы определения конфиденциальности документов объекта защиты;<br>назначение, классификацию и принципы работы специализированного |

| | |
|---|---|
| | оборудования;<br>методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;<br>методы и средства защиты информации в телекоммуникациях от вредоносных программ;<br>технологии применения программных продуктов;<br>возможные способы, места установки и настройки программных продуктов;<br>методы и способы защиты информации, передаваемой по кабельным направляющим системам;<br>конфигурации защищаемых сетей;<br>алгоритмы работы тестовых программ;<br>средства защиты различных операционных систем и среды передачи информации;<br>способы и методы шифрования (кодирование и декодирование) информации. |

**1.3. Количество часов, отводимое на освоение профессионального модуля**

Всего часов: 458 часов, в том числе:
на освоение МДК – 308 часа,
на практики 144 часов, в том числе:
учебную – 72 часа,
производственную – 72 часа.
консультации – 14 часов;
самостоятельную работу – 6 часов;
промежуточная аттестация – 6 часов.