**Аннотация к рабочей программе**

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

**по специальности: 11.02.15 - Инфокоммуникационные сети и системы связи**

**1. Область применения программы**

Программа профессионального модуля (далее рабочая программа) –является частью основной образовательной программы по специальности среднего профессионального обучения 11.02.15 Инфокоммуникационные сети и системы связи в соответствии с ФГОС СПО 11.02.15 Инфокоммуникационные сети и системы связи, утверждённым приказом Министерства образования и науки Российской Федерации 09 декабря 2016 № 1584.

**2**. **Цель и планируемые результаты освоения учебной дисциплины:**

В результате изучения профессионального модуля студент должен освоить основной вид деятельности ПМ.03. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи и соответствующие ему профессиональные компетенции:

|  |  |
| --- | --- |
| **Код** | **Профессиональные компетенции** |
| ВД | 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. Требования к практическому опыту, умениям, знаниям:**

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

**иметь практический опыт в:**

**ПО 1**. выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности;

**ПО 2.** разработка комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;

**ПО 3.** осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения, и оборудования;

**У1.** классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;

**У2.** проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей;

**У3.** определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи;

**У4.** осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;

**У5.** выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты выполнять тестирование систем с целью определения уровня защищенности;

**У6.** определять оптимальные способы обеспечения информационной безопасности;

**У7.** проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях;

**У8.** проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации;

**У9.** разрабатывать политику безопасности сетевых элементов и логических сетей;

**У10.** выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;

**У11.** производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи;

**У12.** конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

**У13.** защищать базы данных при помощи специализированных программных продуктов;

**У14.** защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.

**З1.** принципы построения информационно-коммуникационных сетей;

**З2.** международные стандарты информационной безопасности для проводных и беспроводных сетей;

**З3.** нормативно - правовые и законодательные акты в области информационной безопасности;

**З4.** акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;

**З5.** технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;

**З6.** способы и методы обнаружения средств съёма информации в радиоканале;

**З7.** классификацию угроз сетевой безопасности;

**З8.** характерные особенности сетевых атак;

**З9.** возможные способы несанкционированного доступа к системам связи;

**З10.** правила проведения возможных проверок согласно нормативных документов ФСТЭК;

**З11.** этапы определения конфиденциальности документов объекта защиты;

**З12.** назначение, классификацию и принципы работы специализированного оборудования;

**З13.** методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP, WPA и WPA 2;

**З14.** методы и средства защиты информации в телекоммуникациях от вредоносных программ;

**З15.** технологии применения программных продуктов;

**З16.** возможные способы, места установки и настройки программных продуктов;

**З17.** методы и способы защиты информации, передаваемой по кабельным направляющим системам;

**З18.** конфигурации защищаемых сетей;

**З19.** алгоритмы работы тестовых программ;

**З20.** средства защиты различных операционных систем и среды передачи информации;

**З21.** способы и методы шифрования (кодирование и декодирование) информации.

**4. Количество часов на освоение программы учебной дисциплины:**

Всего **– 612** часов,

* на освоение МДК 03.01 – 144 часа, включая самостоятельную работу – 20 часов,
* на освоение МДК 03.02 – 216 часа, включая самостоятельную работу – 20 часа,
* учебной практики УП 03.01 – 72 часа,
* производственной практики ПП.01 – 180 часов.

**5.Тематический план**

**МДК 03.01**Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи.

**Тема 1.1.**Основы безопасности информационных технологий**.**

**Тема 1.2.**Обеспечение безопасности информационных технологий.

**Тема 1.3.** Средства защиты информации от несанкционированного доступа.

**Тема 1.4.** Обеспечение безопасности компьютерных систем и сетей.

**МДК 03.02** Устройство наливных стяжек пола вручную и механизированным способом.

**Тема 2.1.** Основы информационной безопасности.

**Тема 2.2.** Организационно правовые аспекты защиты информации.

**Тема 2.3.** Комплексная система защиты информации.

**Тема 2.4.** Инженерно-техническая защита информации.

**Тема 2.5.** Криптографическая защита информации.

**Тема 2.6.** Аттестация и лицензирование объектов защиты.

**Учебная практика** УП.03.01 Выполнение работ по обеспечению информационной безопасности.

**Производственная практика ПП.01** Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи.

**6. Промежуточная аттестация:**

**МДК 03.01** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи – экзамен;

**МДК 03.02** Устройство наливных стяжек пола вручную и механизированным способом – дифференцированный зачет;

**Учебная практика** Выполнение работ по обеспечению информационной безопасности - дифференцированный зачет;

**Производственная практика** Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи - дифференцированный зачет.