**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ, ВХОДЯЩЕЙ В ОБРАЗОВАТЕЛЬНУЮ ПРОГРАММУ**

**11.02.08 СРЕДСТВА СВЯЗИ С ПОДВИЖНЫМИ ОБЪЕКТАМИ (базовый уровень)**

**профессиональный модуль ПМ.03 Обеспечение информационной безопасности систем мобильной связи**

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

освоение вида деятельности: «Обеспечение информационной безопасности систем мобильной связи»

В результате освоения профессиональногомодуля обучающийся должен **иметь практический опыт:**

* выявления каналов утечки информации;
* определения необходимых средств защиты;
* проведения аттестации объекта защиты (проверки уровня защищенности);
* разработки политики безопасности для объекта защиты;
* установки, настройки специализированного оборудования по защите информации;
* выявления возможных атак на автоматизированные системы;
* установки и настройки программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;
* конфигурирования автоматизированных систем и информационно-коммуникационных сетей;
* проверки защищенности автоматизированных систем и информационно-коммуникационных сетей;
* защиты баз данных;
* организации защиты в различных операционных системах и средах;
* шифрования информации.

В результате освоения профессиональногомодуля обучающийся должен **уметь**:

* классифицировать угрозы информационной безопасности;
* проводить выбор средств защиты в соответствии с выявленными угрозами;
* определять возможные виды атак;
* осуществлять мероприятия по проведению аттестационных работ;
* разрабатывать политику безопасности объекта:
* использовать программные продукты, выявляющие недостатки систем защиты;
* выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
* производить установку и настройку средств защиты;
* конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности;
* выполнять тестирование систем с целью определения уровня защищенности;
* использовать программные продукты для защиты баз данных;
* применять криптографические методы защиты информации.

В результате освоения профессиональногомодуля обучающийся должен **знать:**

* каналы утечки информации;
* назначение, классификацию и принципы работы специализированного оборудования;
* принципы построения информационно-коммуникационных сетей;
* возможные способы несанкционированного доступа;
* законодательные и нормативные правовые акты в области информационной безопасности;
* правила проведения возможных проверок;
* этапы определения конфиденциальности документов объекта защиты;
* технологии применения программных продуктов;
* возможные способы, места установки и настройки программных продуктов;
* конфигурации защищаемых сетей;
* алгоритмы работы тестовых программ;
* средства защиты различных операционных систем и сред;
* способы и методы шифрования информации.

**Место профессионального модуля в структуре основной профессиональной образовательной программы:** Профессиональный модуль основной профессиональной образовательной программы.

**Требования к уровню освоения содержания профессионального модуля.**

Процесс изучения профессионального модуля направлен на формирование у обучающегося следующих компетенций:

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

ПК 3.1. Использовать программно-аппаратные средства защиты информации в системах мобильной связи.

ПК 3.2. Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.

ПК 3.3. Обеспечивать безопасное администрирование систем и сетей.