**АННОТАЦИЯ**

**РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ 03 Обеспечение информационной безопасности в телекоммуникационных системах и сетях вещания**

**1.1. Область применения программы**

Рабочая программа профессионального модуля является частью основной профессиональной образовательной программы в соответствии с ФГОС по специальности СПО 11.02.10 Радиосвязь, радиовещание и телевидение в части освоения основного вида профессиональной деятельности (ВПД) техническая эксплуатация информационно-коммуникационных сетей связи и вещания и соответствующих профессиональных компетенций (ПК):

1. Использовать программно-аппаратные средства защиты информации в системах радиосвязи и вещания.

2. Применять системы анализа защищенности для обнаружения уязвимостей в сетевой инфраструктуре, давать рекомендации по их устранению.

3. Обеспечивать безопасное администрирование сетей вещания.

**1.2. 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:

иметь практический опыт:

* выявления каналов утечки информации;
* определения необходимых средств защиты;
* проведения аттестации объекта защиты (проверки уровня защищенности);
* разработки политики безопасности для объекта защиты;
* 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;

уметь:

* классифицировать угрозы информационной безопасности;
* проводить выборку средств защиты в соответствии с выявленными угрозами;
* определять возможные виды атак:
* осуществлять мероприятия по проведению аттестационных работ;
* разрабатывать политику безопасности объекта;
* выполнять расчет и установку специализированного оборудования для максимальной защищенности объекта;
* использовать программные продукты, выявляющие недостатки систем защиты;
* 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;

знать:

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

**1.3. Рекомендуемое количество часов на освоение рабочей программы профессионального модуля:**

всего (максимальная учебная нагрузка обучающегося и практика) – 513 часов, включая:

обязательной аудиторной учебной нагрузки обучающегося – 342 часа;

* самостоятельной работы обучающегося – 171 час;

- производственная практика – 36 часов.

**1.4 Содержание профессионального модуля:**

**Раздел 1. Применение комплексной системы защиты информации**

**МДК.03.01**Технология применения комплексной системы защиты информации в системах радиосвязи и сетях вещания

Тема 1.1 Обеспечение безопасности операционных систем

Тема 1.2. Технологии межсетевых экранов

Тема 1.3 Технологии защиты на прикладном уровне

**Тема 1.4.** Каналы утечки информации

**Тема 1.5. Т**ехнологии защищенности и обнаружения атак в системах радиосвязи

**Тема 1.6.** Управление безопасностью в системах радиосвязи

**Тема 1.7.** Основы технологии виртуальных защищенных сетей

**Раздел 2. Применение программно-аппаратных средств защиты информации и систем условного доступа в системах радиосвязи и вещания**

**МДК.02.02. Методы настройки и регулировки устройств и блоков радиоэлектронных приборов**

Тема 2.1 Методы настройки и регулировки радиопередающих устройств

Тема 2.2. Методы настройки и регулировки радиоприемных устройств

Тема 2.3 Измерение параметров систем магнитной и оптической записи информации

Тема 2.4 Измерение параметров элементов системы телевизионного вещания

**Раздел 3. Изучение методов проведения стандартных и сертифицированных испытаний**

**МДК.03.02.**Технология использования систем условного доступа в сетях вещания

**Тема 2.1.** Основные понятия и направления обеспечения информационной безопасности

**Тема2.2.**Правовые основы и стандарты информационной безопасности

**Тема 2.3.** Принципы и алгоритмы криптографической защиты информации в системах радиосвязи

**Тема 2.4.** Основные понятия и принципы функционирования системы условного доступа в сетях вещания