АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи

название профессионального модуля

1.Область применения программы

Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО **11.02.09 Многоканальные телекоммуникационные системы,** входящей в укрупненную группу специальностей **11.00.00 Электроника, радиотехника и системы связи.**

Рабочая программа учебной дисциплины может быть использована в дополнительном профессиональном образовании и в программах профессиональной подготовки обучающихся укрупненной группы специальностей **11.00.00 Электроника, радиотехника и системы связи**в части освоения основного вида деятельности (ВД):

Обеспечение информационной безопасности многоканальных коммуникационных систем и сетей электросвязи

и соответствующих профессиональных компетенций (ПК):

3.1	Использовать программно-аппаратные средства защиты информации в телекоммуникационных систем и сетей связи.
3.2	Применять системы анализа защищенности для обнаружения уязвимости в сетевой инфраструктуре, выдавать рекомендации по их устранению.
3.3	Обеспечивать безопасное администрирование телекоммуникационных систем и информационно-коммуникационных сетей связи.

Рабочая программа профессионального модуля может быть использована в дополнительном образовании в рамках подготовки специалистов по курсу «Обеспечение информационной безопасности многоканальных телекоммуникационных систем и сетей электросвязи».

2.Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля

В результате освоения профессионального модуля 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;

-выявление 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 профессионального модуля 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 системы с целью определения уровня защищенности;
-использовать программные продукты для защиты базы данных;
-применять криптографические методы защиты информации;

В результате освоения профессионального модуля обучающийся должен 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;
-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.

3. Количество часов на освоение профессионального модуля:

Всего - 172 часов, в том числе:
максимальной учебной нагрузки обучающегося - 132 часа
обязательной аудиторной учебной нагрузки обучающегося - 96 часов
самостоятельной работы обучающегося - 40 часа
учебной практики - 36 часов

4. Содержание профессионального модуля

Раздел 1. Владение технологией применения программно-аппаратных средств защиты информации в многоканальных телекоммуникационных системах и сетях электросвязи

Тема 1.1 Конфигурирование защищаемых сетей
Тема 1.2 Собственные средства защиты различных операционных систем и сред
Тема 1.3 Технологии применения программных продуктов. Возможные способы, места установки и настройки программных продуктов.
Тема 1.4 Возможные способы несанкционированного доступа

Тема 1.5 Назначение. Классификация и принципы работы специализированного оборудования.

Тема 1.6 Каналы утечки информации

Раздел 2. Владение технологией применения комплексной системы защиты информации

Тема 2.1 Нормативно-правовые и законодательные акты в области информационной безопасности

Тема 2.2 Принципы построения информационно-коммуникационных сетей

Тема 2.3 Способы и методы шифрования информации

Тема 2.4 Этапы определения конфиденциальности документов объекта защиты

Тема 2.5 Правила проведения возможных проверок. Алгоритмы работы тестовых программ

Учебная практика

1. Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. Выявление каналов утечки информации;

Определение необходимых средств защиты; Проведения аттестации объекта защиты (проверки уровня защищенности);

2. Разработка политики безопасности для объекта защиты;

Установка, настройка специализированного оборудования по защите информации;

3. Выявление возможных атак на автоматизированные системы;

4. Установка и настройка программных средств защиты автоматизированных систем и информационно-коммуникационных сетей;

5. Конфигурирование автоматизированных систем и информационно-коммуникационных сетей; Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей;

6. Защиты баз данных; Организация защиты в различных операционных системах и средах; Шифрование информации.

Оформление отчета. Подготовка к экзамену