**Аннотация рабочей программы профессионального модуля**

|  |
| --- |
| Обеспечение информационной безопасности телекоммуникационных систем |
| и информационно-коммуникационных сетей связи |

*название профессионального модуля*

**1. Область применения программы**

|  |
| --- |
| Рабочая программа учебной дисциплины является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО [**11.02.11 Сети связи и системы коммутации**](http://ugkr.ru/student/ucheb_metod_portal/usheb_mat_metod_ukazaniya_SS.php)**,** 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 телекоммуникационных систем |
| и информационно-коммуникационных сетей связи |

и соответствующих профессиональных компетенций (ПК):

|  |  |
| --- | --- |
| 2.1 | Использовать программно-аппаратные средства защиты информации |
|  | в телекоммуникационных систем и сетей связи. |
| 2.2 | Применять системы анализа защищенности для обнаружения |
|  | уязвимости в сетевой инфраструктуре, выдавать рекомендации по их |
|  | устранению. |
| 2.3 | 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 телекоммуникационных систем и информационно-коммуникационных сетей связи» на базе среднего (полного) общего образования. Опыт работы не требуется.

Рабочая программа составляется для очной, заочной, заочной с элементами дистанционных образовательных технологий формы обучения.

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

В результате освоения профессионального модуля обучающийся должен иметь практический опыт:

- выявление каналов утечки информации;

- определение 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 информационно-коммуникационные сети в соответствии с политикой информационной безопасности;

- выполнять тестирование системы 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 программы профессионального модуля**

Всего – 202 часов, в том числе:

максимальной учебной нагрузки обучающегося – 166 часа, включая:

обязательной аудиторной учебной нагрузки обучающегося – 112 часов;

самостоятельной работы обучающегося – 54 часа;

учебной практики – 36 часов.

**4. Содержание профессионального модуля**

**Раздел 1.** Владение технологией применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи

**МДК 01.** Технология применения программно-аппаратных средств защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи

**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 в телекоммуникационных системах и информационно-коммуникационных сетях связи

**МДК 02.** Технология применения комплексной системы защиты информации в телекоммуникационных системах и информационно-коммуникационных сетях связи

**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

**Тема 2.6**Алгоритма работы тестовых программ

**Учебная практика**

Выявление каналов утечки информации;

Определение необходимых средств защиты;

Проведения аттестации объекта защиты (проверки уровня защищенности);

Разработка политики безопасности для объекта защиты;

Установка, настройка специализированного оборудования по защите информации;

Выявление возможных атак на автоматизированные системы;

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

Конфигурирование автоматизированных систем и информационно-коммуникационных сетей;

Проверка защищенности автоматизированных систем и информационно-коммуникационных сетей;

Защита баз данных;

Организация защиты в различных операционных системах и средах;

Шифрование информации;