**Аннотация рабочей программы профессионального модуля**

|  |
| --- |
| ПМ3. Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи |

*название профессионального модуля*

**1. Цель и планируемые результаты освоения профессионального модуля**

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Обеспечение информационной безопасности инфокоммуникационных сетей и систем связи» и соответствующие ему профессиональные компетенции и общие компетенции:

Перечень общих компетенций

|  |  |
| --- | --- |
| **Код** | **Наименование общих компетенций** |
| ОК 01 | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. |
| ОК 02 | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. |
| ОК 03 | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 04 | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 05 | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 06 | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей. |
| ОК 07 | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 08 | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 09 | Использовать информационные технологии в профессиональной деятельности. |
| ОК 10 | Пользоваться профессиональной документацией на государственном и иностранном языке. |

Перечень профессиональных компетенций

|  |  |
| --- | --- |
| **Код** | **Наименование видов деятельности и профессиональных компетенций** |
| ВД 1 | 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. |

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 17,18

В результате освоения профессионального модуля студент должен:

|  |  |
| --- | --- |
| Иметь практический опыт в: | - анализе сетевой инфраструктуры;  выявлении угроз и уязвимости в сетевой инфраструктуре;  разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;  осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;  использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи. |
| Уметь: | классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;  определять оптимальные способы обеспечения информационной безопасности;  осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;  выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов  выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;  защищать базы данных при помощи специализированных программных продуктов. |
| Знать: | принципы построения информационно-коммуникационных сетей;  международные стандарты информационной безопасности;  акустические и виброакустические каналы утечки информации, особенности их возникновения, организации, выявления, и закрытия;  технические каналы утечки информации, реализуемые в отношении объектов информатизации и технических средств предприятий связи, способы их обнаружения и закрытия;  классификацию угроз сетевой безопасности;  методы и способы защиты информации, передаваемой по кабельным направляющим системам;  правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю;  средства защиты различных операционных систем и среды передачи информации. |

**2. Количество часов на освоение программы профессионального модуля**

Всего часов – 482 часа, в том числе:

- 122 часа вариативной части, направленных на усиление обязательной части программы профессионального модуля.

- учебной практики – 72 часа

- производственной практики –72 часа

- промежуточная аттестация (экзамен (квалификационный)) –8 часов.

**3. Содержание профессионального модуля**

**Раздел ПМ02. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**

**МДК 03.01 Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи**

Тема 1.1. Обеспечение безопасности операционных систем

Тема 1.2 Обеспечение безопасности информационных технологий

Тема 1.3. Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP).

**Учебная практика Корпоративная защита от внутренних угроз информационной безопасности**

**Виды работ**

Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. Разработка маркетингового плана продвижения услуг связи. Выявление конкурентного преимущества на рынке. Проведение маркетингового исследования рынка услуг связи/ Анализ внешней микросреды маркетинга

Ознакомление, подключение, настройка DLP системы Infowatch

Создание стенда виртуальной сети. Установка Traffic Monitor

Подключение компьютеров в домен, установка политик

Установка Device Monitor, Агента на Windows 10

Администрирование Traffic Monitor, установка лицензии, настройка плагинов и политик

Настройка агентских политик на ARM

Настройка политик на Device Monitor

Настройка политик на Traffic Monitor

Создание инцидентов на Traffic Monitor

Создание сводок на Traffic Monitor

Создание отчетов на Traffic Monitor

Анализ выявленных инцидентов и отчетов

Изучение и настройка захвата сетевых хранилищ

Оформление отчета. Участие в зачет-конференции по учебной практике

**Производственная практика**

Участие в создании комплексной системы защиты на предприятии.

Применение программно-аппаратных средств защиты информации на предприятии

Применение инженерно-технических средств защиты информации на предприятии.

Применение криптографических средств защиты информации на предприятии.