АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами

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 2.	*Защита информации в автоматизированных системах программными и программно-аппаратными средствами*
ПК 2.1.	Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.
ПК 2.2.	Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.
ПК 2.3.	Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.
ПК 2.4.	Осуществлять обработку, хранение и передачу информации ограниченного доступа.
ПК 2.5.	Уничтожать информацию и носители информации с

	использованием программных и программно-аппаратных средств.
ПК 2.6.	Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

В ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 15,18

В результате освоения профессионального модуля студент должен:

Иметь практический опыт в	− установки, настройки программных средств защиты информации в автоматизированной системе; − обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; − тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации; − решения задач защиты от НСД к информации ограниченного доступа с помощью программных и программно-аппаратных средств защиты информации; − применения электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных; − учёта, обработки, хранения и передачи информации, для которой установлен режим конфиденциальности; − работы с подсистемами регистрации событий; − выявления событий и инцидентов безопасности в автоматизированной системе.
уметь	− устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; − устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; − диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; − применять программные и программно-аппаратные средства для защиты информации в базах данных; − проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; − применять математический аппарат для выполнения криптографических преобразований;

	– использовать типовые программные криптографические средства, в том числе электронную подпись; – применять средства гарантированного уничтожения информации; – устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; – осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак
знать	– особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; – методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; – типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; – основные понятия криптографии и типовых криптографических методов и средств защиты информации; – особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; – типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.

2. Количество часов на освоение программы профессионального модуля

Всего часов – 802 часа, в том числе:

- 205 часа вариативной части, направленных на усиление обязательной части программы профессионального модуля.
- курсовая работа –30 часов
- учебной практики – 108 часа
- производственной практики –252 часа
- промежуточная аттестация (экзамен (квалификационный)) –7 часов.

3. Содержание профессионального модуля

Раздел ПМ02. Применение программных и программно-аппаратных средств защиты информации

МДК.2.1 Программные и программно-аппаратные средства защиты информации

Тема 1.1. Защищенная автоматизированная система

Тема 1.2 Дестабилизирующее воздействие на объекты защиты

Тема 1.3. Принципы программно-аппаратной защиты информации от несанкционированного доступа

Тема 2.1.
Основы защиты автономных автоматизированных систем
Тема 2.2.Защита программ от изучения
Тема 2.3. Вредоносное программное обеспечение
Тема 2.4. Защита программ и данных от несанкционированного копирования
Тема 2.5. Защита информации на машинных носителях
Тема 2.6. Аппаратные средства идентификации и аутентификации пользователей
Тема 2.7. Системы обнаружения атак и вторжений
Тема 3.1. Основы построения защищенных сетей
Тема 3.2. Средства организации VPN
Тема 4.1.Обеспечение безопасности межсетевого взаимодействия
Тема 5.1. Защита информации в базах данных
Тема 6.1. Изучение мер защиты информации в информационных системах
Тема 6.2. Изучение современных программно-аппаратных комплексов

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.