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 1.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам
ОК 2.	Использовать современные средства поиска, анализа и интерпретации информации, и информационные технологии для выполнения задач профессиональной деятельности
ОК 3.	Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях
ОК 4.	Эффективно взаимодействовать и работать в коллективе и команде
ОК 5.	Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста
ОК 6.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения
ОК 7.	Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях
ОК 8.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности
ОК 9.	Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

Перечень профессиональных компетенций

Код	**Наименование видов деятельности и профессиональных компетенций**
ВД 3	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	- анализировать сетевую инфраструктуру; - выявлять угрозы и уязвимости в сетевой инфраструктуре, - разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи, - осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи - использовать специализированное программное обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.
уметь	- классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи; - проводить анализ угроз и уязвимостей сетевой безопасности IP-сетей, беспроводных сетей, корпоративных сетей; - определять возможные сетевые атаки и способы несанкционированного доступа в конвергентных системах связи; - осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки; - выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продукты - выполнять тестирование систем с целью определения уровня защищенности, - определять оптимальные способы обеспечения информационной безопасности; - проводить выбор средств защиты в соответствии с выявленными угрозами в инфокоммуникационных сетях, - проводить мероприятия по защите информации на предприятиях связи, обеспечивать их организацию, определять способы и методы реализации; - разрабатывать политику безопасности сетевых элементов и логических сетей; - выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей; - производить установку и настройку средств защиты операционных систем, инфокоммуникационных систем и сетей связи; - конфигурировать автоматизированные системы и информационно-коммуникационные сети в соответствии с политикой информационной безопасности; - защищать базы данных при помощи специализированных программных продуктов; - защищать ресурсы инфокоммуникационных сетей и систем связи криптографическими методами.
знать	- принципы построения информационно-коммуникационных сетей; - международные стандарты информационной безопасности для проводных и беспроводных сетей;

	- нормативно - правовые и законодательные акты в области 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; - способы и методы обнаружения средств съёма информации в радиоканале; - классификацию угроз сетевой безопасности; - характерные особенности сетевых атак; - возможные способы несанкционированного доступа к системам связи, - правила проведения возможных проверок согласно нормативным документам ФСТЭК; - этапы определения конфиденциальности документов объекта защиты; назначение, классификацию и принципы работы специализированного оборудования; - методы и способы защиты информации беспроводных логических сетей от НСД посредством протоколов WEP. WPA и WPA 2; - методы и средства защиты информации в телекоммуникациях от вредоносных программ; - технологии применения программных продуктов; - возможные способы, места установки и настройки программных продуктов, - методы и способы защиты информации, передаваемой по кабельным направляющим системам; конфигурации защищаемых сетей; - алгоритмы работы тестовых программ; - средства защиты различных операционных систем и среды передачи информации; - способы и методы шифрования (кодирование и декодирование) информации.

2. Количество часов на освоение программы профессионального модуля

Всего часов – 228 часов, в том числе:

- 24 часа вариативной части, направленных на усиление обязательной части программы профессионального модуля.
- учебной практики – 36 часов
- производственной практики –72 часа
- промежуточная аттестация (экзамен (квалификационный)) –11 часов.

3. Содержание профессионального модуля

Раздел ПМ03. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

МДК 03.01 Защита информации в инфокоммуникационных системах и сетях связи

Тема 1.1 Основы безопасности информационных технологий

Тема 1.2 Обеспечение безопасности информационных технологий

Тема 1.3 Обеспечение безопасности стандартными средствами защиты
Тема 1.4 Криптографическая защита информации

Учебная практика
Подключение, установка стенда, виртуальной машины ТМ.
Подключение, установка драйверов, настройка виртуальной машины агента
Подключение, настройка DLP системы Infowatch
Настройка агентских политик на ARM
Настройка политик на Device Monitor
Настройка политик на Traffic Monitor
Выполнение заданий, настройка агентских политик на ARM
Выполнение заданий, настройка политик на Device Monitor
Выполнение заданий, настройка политик на Traffic Monitor
Оформление отчета. Защита отчета 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.
Оформление отчета. Защита отчета по производственной практике