АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ

1.1. 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 результате освоения профессионального модуля студент должен:

Иметь практический опыт:	- выявления угроз и уязвимостей в сетевой инфраструктуре с использованием системы анализа защищенности; - разработки комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи; - осуществления текущего администрирования для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования.
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 нормативных документов

	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.*

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов – 482 часа, в том числе:

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

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Коды профессиональных общих компетенций	Наименования разделов профессионального модуля	Суммарный объем нагрузки, час.	Объем профессионального модуля, час.					Самостоятельная работа [1]
			Обучение по МДК			*Практики*		
			Всего	*В том числе*		Учебная	Производственная	
				Лабораторных и практических занятий	Курсовых работ (проектов)			
ПК 3.1, 3.3 ОК 01-10	**Раздел 1.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи	**166**	**142**	70	-	-	-	14
ПК 3.1-3.3 ОК 01-10	**Раздел 2.** Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи	**164**	**140**	70		-	-	14
ПК 3.1-3.3 ОК 01-10	Учебная практика *(по профилю специальности), часов (концентрированно)*	**72**				72	-	
ПК 3.1-3.3 ОК 01-10	Производственная практика *(по профилю специальности), часов (Концентрированная) практика)*	**72**					72	
	Промежуточная аттестация (экзамен)							
	Всего:	**330**	**282**	**140**	**-**	**72**	**72**	**28**

[1] *Самостоятельная работа в рамках образовательной программы планируется образовательной организацией в соответствии с требованиями ФГОС СПО в пределах объема профессионального модуля в количестве часов, необходимом для выполнения заданий самостоятельной работы обучающихся, предусмотренных тематическим планом и содержанием профессионального модуля.*

3. Содержание профессионального модуля

Раздел 1. Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

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

Тема 1.1.Основы безопасности информационных технологий
Тема 1.2. Обеспечение безопасности информационных технологий
Тема 1.3. Средства защиты информации от несанкционированного доступа
Тема 1.4. Обеспечение безопасности компьютерных систем и сетей

Раздел 2. Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи

МДК 03.02 Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи

Тема 2.1. Основы информационной безопасности
Тема 2.2. Организационно-правовые аспекты защиты информации
Тема 2.3.Комплексная система защиты информации
Тема 2.4. Инженерно-техническая защита информации
Тема 2.5.Криптографическая защита информации
Тема 2.6.Аттестация и лицензирование объектов защиты

Учебная практика

Виды работ:

- установка, настройка и обслуживание технических средств защиты информации и средств охраны объектов;
- установка и настройка типовых программно-аппаратных средств защиты информации;
- использование программно-аппаратных и инженерно-технических средств.
- настройка, регулировка и ремонт оборудования средств защиты;
- выбор способов и средств многоуровневой защиты телекоммуникационных сетей в соответствии с нормативно-правовой базой;
- проведение типовых операции настройки средств защиты операционных систем;
- проведение аттестации объектов защиты;
- определение источников несанкционированного доступа, исходя из модели угроз;
- определение типа сигнала и технического средства в соответствии с алгоритмом программного продукта;
- обнаружение и обезвреживание разрушающих программных воздействий с использованием программных средств;
- защита телекоммуникационных сетей техническими средствами в соответствии из нормативных документов ФСТЭК;
- защита информации организационными методами в соответствии с инструкциями на объекте.

Итоговый отчёт

Производственная практика

1. Участие в создании комплексной системы защиты на предприятии.
2. Применение программно-аппаратных средств защиты информации на предприятии
3. Применение инженерно-технических средств защиты информации на предприятии.
4. Применение криптографических средств защиты информации на предприятии.

Итоговый отчет