**АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

ПМ02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты

*название профессионального модуля*

## 1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты» 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 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 информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты* |
| ПК 2.1. | Производить установку, настройку, испытания и конфигурирование программных и программно-аппаратных, в том числе криптографических средств защиты информации от несанкционированного доступа и специальных воздействий в оборудование информационно – телекоммуникационных систем и сетей. |
| ПК 2.2. | Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. |
| ПК 2.3. | Осуществлять защиту информации от несанкционированных действий и специальных воздействий в информационно – телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств в соответствии с предъявленными требованиями. |

В результате освоения профессионального модуля студент должен:

| | |
|---|---|
| Иметь практический опыт в | - установка, настройка, испытания и конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;<br>- поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС;<br>- защита информации от НСД и специальных воздействий в ИТКС с использованием программных и программно-аппаратных (в том числе криптографических) средств защиты в соответствии с предъявляемыми требованиями. |
| уметь | - выявлять и оценивать угрозы безопасности информации в ИТКС;<br>- настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>-проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>-выявлять и оценивать угрозы безопасности информации в ИТКС;<br>- проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>- проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>- проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;<br>-выявлять и оценивать угрозы безопасности информации в ИТКС;<br>-настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;<br>-проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>*-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;*<br>*-проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации российского производства.* |
| знать | - способов защиты информации от несанкционированного доступа (далее – НСД) и специальных воздействий на нее;<br>-типовых программных и программно-аппаратных средств защиты информации в ИТКС;<br>-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;<br>-возможных угроз безопасности информации в ИТКС;<br>-способов защиты информации от НСД и специальных воздействий на нее; |

| | |
|---|---|
| | -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;<br>-организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации;<br>-порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;<br>-возможных угроз безопасности информации в ИТКС;<br>- способов защиты информации НСД и специальных воздействий на нее;<br>-типовых программных и программно-аппаратных средств защиты информации в ИТКС;<br>-криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;<br>-порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации<br>*-программные и программно-аппаратные средства защиты информации в ИТКС российского производства;*<br>*-криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС на основе российских стандартов;*<br>*-порядок и правила ведения документации планово предупредительных работ на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.* |

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

Всего часов – 715 часов, в том числе:

- 250 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.
- курсовая работа–30 часов
- учебной практики – 108 часов
- производственной практики – 144 часа
- промежуточная аттестация (экзамен (квалификационный)) – 6 часов.

**3. Содержание профессионального модуля**

**Раздел ПМ02. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты**

**МДК 2.1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты**

Тема 1.1 Обеспечение безопасности операционных систем

Тема 1.2 Технологии разграничения доступа

Тема 1.3 Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN

Тема 1.4 Защита серверных частей виртуальной защищенной сети

Тема 1.5 Технологии обнаружения и предотвращения вторжений

Тема 1.6 Методы управления средствами защиты

**МДК 2.2 Криптографическая защита информации**

Тема 2.1Основы криптографических методов защиты информации

Тема 2.2Современные стандарты шифрования

Тема 2.3 Криптографические методы обеспечения безопасности сетевых технологий

Тема 2.4Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке

**Учебная практика**

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

Подключение, установка драйверов, настройка программных средств шифрования Криптон.

Администрирование программных средств шифрования Криптон

Подключение, установка драйверов, настройка аппаратных средств шифрования Криптон.

Администрирование аппаратных средств шифрования Криптон

Выбор, подключение, настройка межсетевого экрана.

Администрирование межсетевого экрана.

Ознакомление, подключение, настройка системы резервного копирования

Администрирование системы резервного копирования

Ознакомление, подключение, настройка системы антивирусной защиты

Администрирование системы антивирусной защиты

Ознакомление, подключение, настройка СЗИ Рутокен Web.

Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth

Ознакомление, подключение, настройка СЗИ Secret Disk

Изучение и настройка СЗИ КриптоПро CSP.

Ознакомление, подключение, настройка СЗИ КриптоПро ЭП.

Изучение и настройка СЗИ КриптоПро УЦ.

Оформление отчета. Участие в зачет - конференции по учебной практике

**Производственная практика**

Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике.

Подключение, установка драйверов, настройка программных средств абонентского шифрования

Администрирование внедренных средств

Настройка средств электронной подписи

Администрирование средств электронной подписи

Администрирование средств PKI

Участие в организации работ по защите персональных компьютеров на предприятии

Участие в организации работ по защите локальных сетей на предприятии

Участие в организации работ по защите работ в глобальной сети интернет на предприятии

Моделирования угроз, расчет рисков информационной безопасности

Администрирование проводной защищенной локальной сети .

Ознакомление, организация, настройка беспроводной защищенной локальной сети.

Подключение, установка драйверов, настройка программных средств СЗИ КриптоПро Stunnel.

Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Client.

Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Personal Firewall.

Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Coordinator HW.

Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Administrator.

Администрирование СЗИ Рутокен ЭЦП 2.0.

Изучение и настройка СЗИ Рутокен PINPad

Администрирование СЗИ Рутокен Web.

Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth

Администрирование СЗИ Secret Disk

Изучение и настройка СЗИ КриптоПро CSP.

Оформление отчета. Участие в зачет- конференции по производственной практике