***Приложение II.2***

***к программе СПО 10.02.04* *«Обеспечение информационной безопасности телекоммуникационных систем»***

**РАБОЧАЯ ПРОГРАММА**

**ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

**ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты**

**2022**

**Составитель:**

**Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ**

**СОДЕРЖАНИЕ**

|  |  |
| --- | --- |
| 1. Общая характеристика рабочей программы профессионального модуля 2. Структура и содержание профессионального модуля 3. Условия реализация программы профессионального модуля 4. Контроль и оценка результатов освоения профессионального модуля   Приложение 1 |  |

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

|  |
| --- |
| ПМ.02. Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных (в том числе, криптографических) средств защиты |

*наименование профессионального модуля*

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

В результате изучения профессионального модуля студент должен освоить основной вид профессиональной деятельности «Разработка модулей программного обеспечения для компьютерных систем» 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 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 | - установка, настройка, испытания и конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации в оборудовании ИТКС;  - поддержание бесперебойной работы программных и программно-аппаратных (в том числе криптографических) средств защиты информации в ИТКС;  - 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;  - настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  - проводить контроль показателей и процесса функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить восстановление процесса и параметров функционирования программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  - проводить техническое обслуживание и ремонт программно-аппаратных (в том числе криптографических) средств защиты информации;  -выявлять и оценивать угрозы безопасности информации в ИТКС;  -настраивать и применять средства защиты информации в операционных системах, в том числе средства антивирусной защиты;  -проводить конфигурирование программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  *-проводить установку и настройку программных и программно-аппаратных (в том числе криптографических) средств защиты информации российского производства;*  *-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;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -возможных угроз безопасности информации в ИТКС;  -способов защиты информации от НСД и специальных воздействий на нее;  -порядка тестирования функций программных и программно-аппаратных (в том числе криптографических) средств защиты информации;  -организации и содержания технического обслуживания и ремонта программно-аппаратных (в том числе криптографических) средств защиты информации;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации;  -возможных угроз безопасности информации в ИТКС;  - способов защиты информации НСД и специальных воздействий на нее;  -типовых программных и программно-аппаратных средств защиты информации в ИТКС;  -криптографических средств защиты информации конфиденциального характера, которые применяются в ИТКС;  -порядка и правил ведения эксплуатационной документации на программные и программно-аппаратные (в том числе криптографические) средства защиты информации  *-программные и программно-аппаратные средства защиты информации в ИТКС российского производства;*  *-криптографические средства защиты информации конфиденциального характера, которые применяются в ИТКС на основе российских стандартов;*  *-порядок и правила ведения документации планово предупредительных работ на программные и программно-аппаратные (в том числе криптографические) средства защиты информации.* |

**1.2. Количество часов, отводимое на освоение профессионального модуля**

Всего часов – 715 часа, в том числе:

- 250 часов вариативной части, направленных на усиление обязательной части программы профессионального модуля.

**2. СТРУКТУРА и содержание профессионального модуля**

**2.1. Структура профессионального модуля**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Коды профессиональных компетенций** | **Наименования разделов профессионального модуля[[1]](#footnote-1)\*** | **Суммарный объем нагрузки, час** | **Объем профессионального модуля, час** | | | | | | |
| **Обучение по МДК** | | | | **Практика** | | **Промежуточная аттестация** |
| **Всего,**  часов | **в т.ч. лабораторные работы и практические занятия,**  часов | **в т.ч., курсовая работа (проект),**  часов | **Самостоятельная работа** | **Учебная,**  часов | **Производственная (по профилю специальности),**часов |
| **ПК 2.1**  **ПК 2.2** | **Раздел 1.** Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты | **273** | **244** | 112 | 20 | **17** |  |  | **12** |
| **ПК 2.3** | **Раздел 2.** Методы криптографической защиты информации | **184** | **162** | 76 | 10 | **14** |  |  | **8** |
| **ПК 2.1-ПК 2.3** | **Учебная практика** |  |  | | | | **108** |  |  |
| **ПК 2.1-ПК 2.3** | **Производственная практика (по профилю специальности)**, часов |  |  | | | |  | **144** |  |
|  | **Промежуточная аттестация (экзамен (квалификационный)) – демонстрационный экзамен** |  |  |  |  |  |  |  | **6** |
|  | **Всего:** |  |  |  |  |  |  | **715** |  |

# 2.2. Тематический план и содержание профессионального модуля (ПМ)

IV семестр

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)** | | **Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся , курсовая работ (проект)** | | | **Объем часов** | |
| **1** | | **2** | | | **3** | |
| Раздел 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты | | | | | 273 | |
| МДК.2.1 Защита информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных средств защиты | | | | | 128 | |
| **Тема 1.1**  Обеспечение безопасности операционных систем | | **Содержание** | | | **26** | |
| 1 | | Вводная лекция. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | |
| 2 | | Основы информационной безопасности | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 73-76 | | |
| 3 | | Проблемы безопасности ОС. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 77-80 | | |
| 4 | | Технологии: идентификации, аутентификации, авторизации. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 81-82 | | |
| 5 | | Архитектура подсистемы защиты. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 83-86 | | |
| 6 | | Разграничение доступа. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 87-90 | | |
| 7 | | Файловая система Windows. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 91-96 | | |
| 8 | | АПМДЗ. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 97-100 | | |
| 9 | | RAID. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр.110-112 | | |
| 10 | | Загрузка операционной системы Windows. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 113-115 | | |
| 11 | | Виртуализация. | 2 | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 116-118 |  | |
| 12 | | Физический уровень. | 2 | |
|  | | **Домашнее задание:** чтение и анализ литературы [1] стр. 120-122 | | |
| 13 | | Защита на физическом уровне. | 2 | |
|  | | **Домашнее задание:** чтение и анализ литературы [1] стр. 123-125 | | |
| **Практические занятия** | | | 26 | |
| 1 | | Обзор VMware Workstation Pro. |
| 2 | | Установка виртуальной машины (Windows 10). |
| 3 | | Редактор реестра в Windows. |
| 4 | | Редактор локальной групповой политики в Windows. |
| 5 | | Службы в Windows. |
| 6 | | Управление дисками в Windows. |
| 7 | | Диспетчер задач в Windows. |
| 8 | | Просмотр событий в Windows. |
| 9 | | Планировщик заданий в Windows. |
| 10 | | Монитор стабильности системы в Windows. |
| 11 | | Системного монитора в Windows. |
| 12 | | Монитор ресурсов в Windows. |
| 13 | | Брандмауэр в Windows. |
| **Самостоятельная работа** | | | **3** | |
| Подготовить выступление на тему «Уязвимости в операционной системе Windows». | | |
| **Тема 1.2**  Обеспечение информационной безопасности сетей. Основы технологии виртуальных защищенных сетей VPN | | **Содержание** | | | **36** | |
| 1 | | Введение в Active Directory. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 123-125 | | |
| 2 | | Канальный уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 126-129 | | |
| 3 | | Защита на канальном уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 130-131 | | |
| 4 | | Протокол DHCP. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 132-135 | | |
| 5 | | Сетевой уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [2] стр. 123-125 | | |
| 6 | | Защита на сетевом уровне. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [3] стр. 123-125 | | |
| 7 | | Протоколы IPv4 и IPv6. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [4] стр. 123-125 | | |
| 8 | | Транспортный уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [2] стр. 123-125 | | |
| 9 | | Защита на транспортном уровне. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [3] стр. 123-125 | | |
| 10 | | Сеансовый уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [4] стр. 123-125 | | |
| 11 | | Защита на сеансовом уровне. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 86-89 | | |
| 12 | | Протокол SSL. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [2] стр. 123-125 | | |
| 13 | | Уровень представления. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [3] стр. 123-125 | | |
| 14 | | Защита на уровне представления. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [4] стр. 123-125 | | |
| 15 | | Прикладной уровень. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | |
| 16 | | Защита на Прикладном уровне. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [2] стр. 123-125 | | |
| 17 | | Протокол DNS. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [3] стр. 123-125 | | |
| 18 | | Протокол VPN. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [4] стр. 123-125 | | |
| **Практические занятия** | | | | **18** |
| 14 | | Установка виртуальной машины (Windows Server 2022). | |
| 15 | | Обзор Windows Admin Center. | |
| 16 | | Развертывание роли DNS в Windows Server. | |
| 17 | | Развертывание роли DHCP в Windows Server. | |
| 18 | | Развертывание основного контролера домена Active Directory в Windows Server. | |
| 19 | | Развертывание дополнительного контроллера домена в существующий домен Active Directory в Windows Server. | |
| 20 | | Обзор управлений пользовательскими и служебными учетными записями в Windows Server. | |
| 21 | | Обзор введения пользователя в домен. | |
| 22 | | Развертывание инфраструктуры групповых политик в Windows Server. | |
| 23 | | Развертывание роли Web Server IIS в Windows Server. | |
| **Самостоятельная работа** | | | | **2** |
| Подготовить выступление на тему «Уязвимости в операционной системе Windows server». | | | |
| **Тема 1.3**  Технологии разграничения доступа | | **Содержание** | | | | **6** |
| 1 | | Введение в командную оболочку Windows PowerShell. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |
| 2 | | Протоколы аутентификации и доступа. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [3] стр. 123-125 | | |
| 3 | | Межсетевой экран. | | 2 |
| **Домашнее задание:** чтение и анализ литературы [4] стр. 123-125 | | |
| **Практические занятия** | | | | **8** |
| 24-27 | | Основные возможности командной оболочки Windows PowerShell. | |  |
| 28-31 | | Введение в язык программирования командной оболочки Windows PowerShell. | |
| **Самостоятельная работа** | | | | **3** |
| Подготовить скрипт при помощи командной оболочки Windows PowerShell, для автоматизации работы на тему «Настройка сети» в операционной системе Linux. | | | |  |
|  | **V семестр** | | | | | **145** |
| **Тема 1.4** Защита серверных частей виртуальной защищенной сети | **Содержание** | | | | | **44** |
| 1,  2 | | **Технология VipNet**  VPN, Туннель, PKI | | | 4 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 172-189 | | | |
| 3,  4,  5 | | **Ключевая структрура**  Шифрования в технологии VipNet | | | 6 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 199-201 | | | |
| 6,  7,  8 | | **Межсетевое взаимодействие**  Технология «Открытый интернет» Координатор Открытого интернета. VipNet клиенты Открытого Интернета. | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 202-210 | | | |
| 9,  10 | | **ViPNet Coordinator**  Функции ViPNet Coordinator 4.х | | | 4 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 103-110 | | | |
| 11 | | **ViPNet Client 4**  ФункцииViPNet Client | | |  |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 250-272 | | | |
| **Самостоятельная работа** | | | | | **9** |
| Подготовить выступление на тему «VipNet». | | | | |  |
| **Практические занятия** | | | | | **22** |
| 31-32 | | Настройка сетевого окружения и компонентов систем | | | 4 |
| 33-34 | | Установка по vipnet administrator для создания защищённой сети | | | 4 |
| 35-36 | | Установка по vipnet coordinator и по vipnet client на соответствующие виртуальные машины | | | 4 |
| 37-38 | | Защита локально-вычислительной сети предприятия с применением по vipnet | | | 4 |
| 39 -41 | | Создание структуры защищенной сети:  модификация защищенной сети  компрометация узла защищенной сети | | | 6 |
| **Тема 1.5**  Технологии обнаружения и предотвращения вторжений | **Содержание** | | | | | **48** |
| 1 | | **DLP система обнаружения внутренних угрох**  Infowatch | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 273-277 | | | |
| 2 | | **Средства анализа защищенности сетевых протоколов и сервисов**  Средства анализа защищенности операционной системы. Общие требования к выбираемым средствам анализа защищенности | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 278-279 | | | |
| 3,4 | | **Средства обнаружения сетевых атак**  Методы анализа сетевой информации. Классификация систем обнаружения атак. Компоненты и архитектура системы обнаружения атак. Особенности систем обнаружения атак на сетевом и операционном уровнях. Методы реагирования на сетевые атаки  Обзор современных средств обнаружения атак | | | 4 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 280-286 | | | |
| 5 | | **Система обнаружения вторжений (IDS)**  Обнаружение вторжения. Прогноз возможных будущих атак. Сетевое зондирование (сканирование) или другое тестирование для обнаружения уязвимостей целевой системы. Выполнение документирования существующих угроз; | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 287-72 | | | |
| 6 | | **Архитектура IDS**  Сенсорная подсистема, предназначенную для сбора событий, связанных с безопасностью защищаемой сети или системы; Подсистема анализа, предназначенную для выявления сетевых атак и подозрительных действий; Хранилище, в котором накапливаются первичные события и результаты анализа; Консоль управления, позволяющая конфигурировать IDS, наблюдать за состоянием защищаемой системы и IDS, просматривать выявленные подсистемой анализа инциденты. | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 7 | | **Система предотвращения вторжений (IPS)**  Программные и аппаратные решения. Мониторинг сети. Компьютерные системы в реальном времени. | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 8 | | **Технологии защиты от вирусов**  Компьютерные вирусы и проблемы антивирусной защитыцикл вирусов. Основные каналы распространения вирусов и других вредоносных программ | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 9 | | **Способы проникновения в систему**  Классификация. Типы объектов. Вредоносные программы. Вирусы и черви  Троянские программы. Подозрительные упаковщики. Вредоносные утилиты | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 10 | | **Программы поведений**  Adware, Pornware, Riskware. | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 11 | | **Правила поглощения типов. Правила именования**  Malware | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 12 | | **Новые технологии**  Проактивные технологии | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| **Практические занятия** | | | | | **24** |
| 42-44 | | Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз | | | 6 |
| 45-46 | | Разработка политик безопасности в системе корпоративной защиты информации от внутренних угроз | | | 4 |
| 47-48 | | Поиск и предотвращениеинцидентов. Технологии анализа сетевого трафика в системе корпоративной защитыинформации от внутренних угроз | | | 4 |
| 49-50 | | Технологии агентского мониторинга | | | 4 |
| 51-53 | | Анализ выявленных инцидентов | | | 6 |
| **Тема 1.6**  Методы управления средствами защиты | **Содержание** | | | | | **12** |
| 1 | | **Методы управления средствами сетевой защиты**  Задачи управления системой сетевой защиты. Архитектура управления средствами сетевой защиты. Функционирование системы управления средствами защиты | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 2 | | **Аудит безопасности информационной системы.**  Мониторинг безопасности системы. Программные средства проведения аудита безопасности. | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| 3 | | **Обзор современных систем управления сетевой защитой**  Классификация систем защиты. Перспективы и тенденции в развитии систем защиты | | | 2 |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 66-72 | | | |
| **Практические занятия** | | | | | **6** |
| 54-56 | | Nmap | | | 6 |
| **Курсовой проект (работа)** | | | | | | **20** |
| **Промежуточная аттестация (экзамен)** | | | | | | **12** |

IV семестр

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Раздел 2. Методы криптографической защиты информации | | | | 184 |
| МДК 2.2 Криптографическая защита информации | | | | 108 |
| Тема 2.1  Основы криптографических методов защиты информации  . | Содержание | | | 40 |
| 1 | | Свойства информационной безопасности  Свойства информационной безопасности, обеспечиваемые криптографическими методами защиты информации. Виды атак. Службы безопасности и механизмы достижения требуемого уровня защищенности | 2 |
| **Домашнее задание:** чтение и анализ литературы [10] стр. 20 - 25 |
| 2 | | Криптографические методы  Шифрование. Кодирование. Стеганография. Сжатие | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 23- 25 |
| 3 | | Математика криптографии  Бинарные операции. Арифметика целых чисел. Модульная арифметика. Матрицы. Линейное сравнение | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 26-28 |
| 4 | | Традиционные шифры перестановки  Шифры перестановки. Одно и двух направленные. Поточные и блочные шифры. Механизация шифрования | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 25-27 |
| 5 | | Традиционные шифры замены  Шифры замены. Шифры многоалфавитной замены. Частотность символов. | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 27-30 |
| 6 | | Криптоанализ шифров перестановки  Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 30-35 |
| 7 | | Криптоанализ шифров замены  Атака грубой силы. Частотный анализ. Атака по образцу. Атака знания исходного текста | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 36-38 |
| 8,  9 | | Компьютерное шифрование  Кодовая таблица ASCII. Алгебраические структуры: группы, кольца, поля. Генератор паролей | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 36- 37 |
| 10 | | Современная компьютерная стеганография  Контейнеры. Скрытие информации в изображениях, текстовых файлах, видеозаписях. | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 38-45 |
| Практические занятия | | | 20 |
| 57 | | Бинарная арифметика. Модульная арифметика |
| 58 | | Применение методов шифрования перестановкой |
| 59 | | Применение методов шифрования заменой |
| 60 | | Применение методов шифрования многоалфавитной замены |
| 61-62 | | Криптоанализ методов перестановки |
| 63-64 | | Криптоанализ методов замены |
| 65 | | Компьютерное шифрование |
| 66 | | Стеганографические методы скрытия информации |
| Тема 2.2  Современные стандарты шифрования | Содержание | | | 28 |
| 1 | | Симметричное шифрование  Сети Файстеля. Стандарт шифрования данных DES. Структура DES. Анализ DES. Многократное применение DES. Безопасность DES Проблема распределения ключей симметричного шифрования | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр.47 – 50 |
| 2,  3 | | Усовершенствованный стандарт шифрования АЕS  Структура AES. Расширение ключей 128/192/256. Анализ безопасности АЕS Российские стандарты симметричного шифрования | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 51 – 54 |
| 4,  5 | | Асимметричное шифрование RSA  Простые числа и уравнения. Разложение на множители. RSA. Теорема об остатках. | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 55- 57 |
| 6,  7 | | Асимметричное шифрование на основе логарифмов  Возведение в степень и логарифмы. Криптографическая система Эль-Гамаля. Криптосистемы на основе метода эллиптических кривых. ЭЦП. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов Криптосистемы на основе метода эллиптических кривых.  ЭЦП. ГОСТ 34.10-94. ГОСТ Р 34.10-2001. ГОСТ Р 34.10 -2012. Безопасность асимметричных алгоритмов ГОСТ Р 34.12-2015 | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 57- 78 |
| Практические занятия | | | 14 |
| 67 | | Алгоритм Диффи-Хелмана. Организация алгоритма передачи симметричного ключа | 2 |
| 68 | | Ассиметричное шифрование. Алгоритм разложения произведения двух простых чисел на множители | 2 |
| 69 | | Разработка Хэш-функции | 2 |
| 70 | | Разработка схемы простого пароля | 2 |
| 71 | | Сертификаты открытого ключа | 2 |
| 72 | | Настрока и администрирование токена | 2 |
| 73 | | Разработка алгоритма PGP | 2 |
| Тема 2.3  Криптографические методы обеспечения безопасности  сетевых технологий | Содержание | | | 32 |
| 1 | | Целостность сообщения  Случайная модель Огас1е. Установление подлинности сообщения. Криптографические хэш-функции. MD-5. SHA-1. SНА-512. ГОСТ Р 34.11-94. ГОСТ Р 34.11 -2012 Анализ безопасности хэш-функций. Атаки на хэш-функции | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 81-83 |
| 2,  3 | | Электронная цифровая подпись  Алгоритм формирования подписи. Свойства обеспечиваемые ЭЦП. Схемы цифровой подписи. Атаки на цифровую подпись. ЭЦП с временной меткой. Слепая ЭЦП. Бесспорная ЭЦП. ГОСТ Р 34.10 -2012. Установление подлинности объекта  Простой пароль. Динамический пароль. Запрос-ответ. PIN. Подтверждение с нулевым разглашением. Биометрические средства идентификации. Электронные ключи и карты. Токены | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [11] стр. 83-85 |
| 4,  5 | | Проблемы распределения открытого ключа асимметричного шифрования  Сертификаты открытого ключа. Удостоверяющие центры. Х.509. Иерархия PKI Электронная почта. Архитектура e-mail. РGР. S/М1МЕ | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [10] стр. 80-82 |
| 6 | | Обеспечение безопасности сети с применением криптографических протоколов на транспортном и сетевом уровне  Форматы сообщения SSL. TLS. Безопасность транспортного уровня IPSec. Организация VPN-сети | 2 |
|  | | **Домашнее задание:** чтение и анализ литературы [12] стр. 123-125 |
| 7,  8 | | Защита информации в сетях организованных по технологии беспроводного доступа Защита информации в сетях сотовой связи  IEEE 802.11. WEP. WPA. WPA-2. IEEE 802.16 A3. A8.A5/3. Атаки на алгоритмы  Перспективы развития беспроводной мобильной связи | 4 |
|  | | **Домашнее задание:** чтение и анализ литературы [12] стр. 23-25 |
| Практические занятия | | | 16 |
| 74 | Изучение протоколов SSL, TLS, IPSec | | 2 |
| 75 | Настройка безопасности беспроводной сети передачи информации IEEE 802.11. WEP. WPA. WPA-2 | | 2 |
| 76 | Процедура аутентификации пользователя на основе пароля | | 2 |
| 77 | Программная реализация криптографических алгоритмов | | 2 |
| 78 | Механизмы контроля целостности данных | | 2 |
| 79 | Алгоритмы поведения вирусных и других вредоносных программ | | 2 |
| 80-81 | Пакеты антивирусных программ | | 4 |

**V семестр**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Тема 2.4  Средства и услуги в области криптографической защиты информации, представленные на отечественном рынке | | | Содержание | | 52 |
| 1 | Средства криптографической защиты информации «КриптоПро»  Средства криптографической защиты информации. КриптоПро CSP. КриптоПро ЭП. КриптоПро JCP .КриптоПро .NET. КриптоПро IPSec. КриптоПро HSM. Атликс HSM. КриптоПро AirKey | 2 |
|  | **Домашнее задание:** чтение и анализ литературы [7] стр. 23-25 |
| 2 | Средства криптографической защиты информации со смарткартами и USB ключами  КриптоПро CSP для универсальной электронной карты. Магистра CSP. КриптоПро Рутокен CSP. КриптоПро ФКН CSP 3.9. КриптоПро CSP 4.0 ФКН (Gemalto) | 2 |
|  | **Домашнее задание:** чтение и анализ литературы [8] стр. 23-25 |
| 3 | Инфраструктура открытых ключей КриптоПро  Удостоверяющий центр КриптоПро УЦ. КриптоПро TSP. КриптоПро OCSP. КриптоПро SVS. АРМ разбора конфликтных ситуаций. КриптоПро Revocation Provider. КриптоПро ЭЦП. КриптоПро ЭЦП Browser plug-in. КриптоПро SSF  КриптоПро DSS. КриптоПро DSS Lite | 2 |
|  | **Домашнее задание:** чтение и анализ литературы [7] стр. 26-28 |
| 4 | Защита от несанкционированного доступа с использованием КриптоПро CSP  КриптоПро TLS. КриптоПро Stunnel. КриптоПро Winlogon. КриптоПро EAP-TLS  СЗИ Secure Pack Rus 3.0. КриптоПро EFS | 2 |
| **Домашнее задание:** чтение и анализ литературы [8] стр. 26-28 |
| 5 | Системы идентификации Программы и утилиты  IdM. КриптоАРМ (Крипто Три). Приложение командной строки cryptcp  Браузер КриптоПро Fox. ЭЦП процессор. КриптоПро PDF. КриптоПро Office Signature. КриптоПро CRM | 2 |
| **Домашнее задание:** чтение и анализ литературы [7] стр. 29-31 |
| 6 | Клиентские компоненты средств информационной безопасности «Инфотекс»  ViPNet Client. ViPNet Personal Firewall. ViPNet Client Mobile  ViPNet Connect. ViPNet CryptoFile. ViPNet CSP | 2 |
| **Домашнее задание:** чтение и анализ литературы [8] стр. 29-31 |
| 7 | Серверные компоненты средств информационной безопасности «Инфотекс»  ViPNet Coordinator HW. ViPNet Coordinator KB. ViPNet Coordinator Software. ViPNet HSM. ViPNet IDS. ViPNet Industrial Gateway | 2 |
| **Домашнее задание:** чтение и анализ литературы [7] стр. 31-33 |
| 8 | Компоненты управления «Инфотекс»  ViPNet Administrator. ViPNet Statewatcher. ViPNet Certification Authority. ViPNet Policy Manager | 2 |
| **Домашнее задание:** чтение и анализ литературы [8] стр. 31-33 |
| 9 | Криптографическая линейка продуктов компании «Аладдин»  JaCarta. "Антифрод-терминал". JC-WebClient. JaCarta SecurLogon. ПО JaCarta АРМ УЦ. "КриптоПро ФКН CSP" | 2 |
| **Домашнее задание:** чтение и анализ литературы [7] стр. 33-35 |
| 10 | Семейство Secret Disk  Secret Disk Enterprise. Secret Disk Server NG. Secret Disk 5. Сертификаты  Алгоритмы шифрования. Защита 1С:Предприятие | 2 |
| **Домашнее задание:** чтение и анализ литературы [8] стр. 33-35 |
| 11 | НТЦ Атлас  «Атликс-VPN»,«Модуль-HSM». Однонаправленный шлюз «Атликс-Шлюз-К»  Программно-аппаратный комплекс (ПАК) «Криптосервер». Система обнаружения сетевых атак программно-аппаратный комплекс "Тор". Комплексная система голографического и криптографического контроля целостности документов (КСГК) | 2 |
| **Домашнее задание:** чтение и анализ литературы [7] стр. 35-38 |
| 12 | Продукты Рутокен  Рутокен ЭЦП 2.0. Рутокен Lite. Рутокен S. Рутокен ЭЦП 2.0 Flash. Рутокен ЭЦП PKI. Рутокен PINPad. Рутокен ЭЦП Bluetooth. Рутокен Web. Рутокен VPN. Рутокен Плагин. Рутокен для Windows. КриптоТри. Рутокен KeyBox. КриптоПро Рутокен CSP | 2 |
| **Домашнее задание:** чтение и анализ литературы [7] стр. 38-40 |
| 13 | Продукты Анкад  Средства для работы с ключевой информацией Crypton VPN Защищенный тонкий клиент КРИПТОН-ЗАМОК Комплекс аппаратно-программных средств ограничения доступа | 2 |
| **Домашнее задание:** чтение и анализ литературы [8] стр. 40-42 |
| Практические задания | | 26 |
| 82-84 | Изучение средств обнаружения атак | 6 |
| 85-87 | Алгоритмы предупреждения и обнаружения вирусных угроз | 6 |
| 88-90 | Изучение и настройка СЗИ Рутокен Web. | 6 |
| 91-92 | Изучение и настройка СЗИ Рутокен CSP. | 4 |
| 93-94 | Изучение и настройка СЗИ Рутокен Bluethoth. | 4 |
| Самостоятельная работа при изучении раздела ПМ.2  Систематическая проработка конспектов занятий, учебной и специальной технической литературы (по вопросам к параграфам, главам учебных пособий, составленным преподавателем).  Подготовка к практическим работам с использованием методических рекомендаций преподавателя.  Оформление практических работ, отчетов и подготовка к их защите. | | | | | 6 |
| Курсовая работа (проект) | | | | | 10 |
| Промежуточная аттестация (экзамен) | | | | | 8 |
| Примерная тематика курсовых проектов | | | | |  |
|  | Защита информации с применением СЗИ Рутокен S | | | |  |
|  | Защита информации с применением СЗИ Secret Disk | | | |
|  | Защита информации с применением СЗИ КриптоПро CSP | | | |
|  | Защита информации с применением СЗИ КриптоПро ЭП. | | | |
|  | Защита информации с применением СЗИ ViPNet Policy Manager | | | |
|  | Защита информации с применением СЗИ КриптоПро Stunnel. | | | |
|  | Защита информации с применением СЗИ ViPNet Client. | | | |
|  | Защита информации с применением СЗИ ViPNet EndPoint Protection | | | |
|  | Защита информации с применением СЗИ ViPNet Coordinator Windows | | | |
|  | Защита информации с применением с СЗИ ViPNet Administrator | | | |
|  | Защита информации с применением СЗИ Secret Net Studio | | | |
|  | Защита информации с применением СЗИ ViPNet SafeDisk | | | |
|  | Защита информации с применением СЗИ Соболь 4.0 | | | |
|  | Защита информации с применением СЗИ КриптоПро УЦ. | | | |
|  | Защита информации с применением СЗИ ViPNet Coordinator Linux | | | |
|  | Защита информации с применением СЗИ Рутокен Bluetooth | | | |
|  | Защита информации с применением СЗИ Alladin eToken | | | |
|  | Защита информации с применением СЗИ VipPNet CSP | | | |
|  | Защита информации с применением СЗИ JaCarta АРМ УЦ | | | |
|  | Защита информации с применением СЗИ JC-WebClient | | | |
|  | Защита информации с применением СЗИ JaCarta SecurLogon | | | |
|  | Защита информации с применением СЗИ OpenVPN | | | |
|  | Защита информации с применением СЗИ ViPNet EndPoint Protection | | | |
|  | Защита информации с применением СЗИ ViPNet Coordinator HW100C | | | |
|  | Защита информации с применением с СЗИ Соболь 4.0 | | | |
|  | Защита информации с применением СЗИ Рутокен S | | | |
|  | Защита информации с применением СЗИ Secret Disk | | | |
|  | Защита информации с применением СЗИ КриптоПро CSP. | | | |
| Учебная практика 2.01 Вариативно(Корпоративная защита от внутренних угроз информационной безопасности)  Виды работ | | | | | 108 |
| 1 | | 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 | | | 6 |
| 2 | | Ознакомление, подключение, настройка DLP системы Infowatch  Создание стенда виртуальной сети. Установка Traffic Monitor | | | 6 |
| 3 | | Подключение компьютеров в домен, установка политик | | | 6 |
| 4 | | Установка Device Monitor, Агента на Windows 10 | | | 6 |
| 5 | | Администрирование Traffic Monitor, установка лицензии, настройка плагинов и политик | | | 6 |
| 6 | | Настройка агентских политик на ARM | | | 6 |
| 7 | | Настройка политик на Device Monitor | | | 6 |
| 8 | | Настройка политик на Traffic Monitor | | | 6 |
| 9 | | Создание инцидентов на Traffic Monitor | | | 6 |
| 10 | | Создание сводок на Traffic Monitor | | | 6 |
| 11 | | Создание отчетов на Traffic Monitor | | | 6 |
| 12 | | Анализ выявленных инцидентов и отчетов | | | 6 |
| 13 | | Изучение и настройка захвата сетевых хранилищ | | | 6 |
| 14 | | Оформление отчета. Участие в зачет-конференции по учебной практике | | | 6 |
| Учебная практика 2.01 Вариативно(Кибербезопасность)  Виды работ | | | | |  |
| 1 | | Проведение инструктажа по технике безопасности. Ознакомление с планом проведения учебной практики. Получение заданий по тематике. | | | 6 |
| 2 | | Ознакомление с гипервизором VMWare ESXI. Создание групп портов, пользователей, снапшотов. | | | 6 |
| 3 | | Ознакомление, установка, базовая настройка Cisco FirePower и Pfsense | | | 6 |
| 4 | | Ознакомление с маршрутизатором Mikrotik RouterOS. Импортирование, базовая настройка. | | | 6 |
| 5 | | Создание базовой инфраструктуры сети, построение маршрутов в Mikrotik RouterOS. | | | 6 |
| 6 | | Настройка DNS | | | 6 |
| 7 | | Настройка DHCP | | | 18 |
| 8 | | Настройка правил разграничения трафика файервола Cisco FirePower | | | 18 |
| 9 | | Развертывание Active Directory.Создание пользователей | | | 6 |
| 10 | | Поднятие центра сертификации. Выпуск сертификата | | | 6 |
| 11 | | Настройка активной аутентификации | | | 6 |
| 12 | | Проверка работы правил фаейрвола | | | 6 |
| 13 | | Проверка работы активной аутентификации | | | 6 |
| 14 | | Оформление отчета. Участие в зачет-конференции по учебной практике | | | 6 |
| Производственная практика (по профилю специальности) 2.02  Виды работ | | | | | 144 |
| 1 | | Проведение инструктажа по технике безопасности. Ознакомление с предприятием. Получение заданий по тематике. | | | 6 |
| 2 | | Подключение, установка драйверов, настройка программных средств абонентского шифрования | | | 6 |
| 3 | | Администрирование внедренных средств | | | 6 |
| 4 | | Настройка средств электронной подписи | | | 6 |
| 5 | | Администрирование средств электронной подписи | | | 6 |
| 6 | | Администрирование средств PKI | | | 6 |
| 7 | | Участие в организации работ по защите персональных компьютеров на предприятии | | | 6 |
| 8 | | Участие в организации работ по защите локальных сетей на предприятии | | | 6 |
| 9 | | Участие в организации работ по защите работ в глобальной сети интернет на предприятии | | | 6 |
| 10 | | Моделирования угроз, расчет рисков информационной безопасности | | | 6 |
| 11 | | Администрирование проводной защищенной локальной сети . | | | 6 |
| 12 | | Ознакомление, организация, настройка беспроводной защищенной локальной сети. | | | 6 |
| 13 | | Подключение, установка драйверов, настройка программных средств СЗИ КриптоПро Stunnel. | | | 6 |
| 14 | | Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Client. | | | 6 |
| 15 | | Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Personal Firewall. | | | 6 |
| 16 | | Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Coordinator HW. | | | 6 |
| 17 | | Подключение, установка драйверов, настройка программных средств СЗИ ViPNet Administrator. | | | 6 |
| 18 | | Администрирование СЗИ Рутокен ЭЦП 2.0. | | | 6 |
| 19 | | Изучение и настройка СЗИ Рутокен PINPad | | | 6 |
| 20 | | Администрирование СЗИ Рутокен Web. | | | 6 |
| 21 | | Изучение и настройка СЗИ Рутокен ЭЦП Bluetooth | | | 6 |
| 22 | | Администрирование СЗИ Secret Disk | | | 6 |
| 23 | | Изучение и настройка СЗИ КриптоПро CSP. | | | 6 |
| 24 | | Оформление отчета. Участие в зачет- конференции по производственной практике | | | 6 |
|  | | Промежуточная аттестация (квалификационный экзамен) | | | 6 |
| Всего: | | | | | 715 |

# 3. условия реализации программы ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

# 3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля предполагает наличие лаборатории программных и программно-аппаратных средств защиты информации

Оборудование лаборатории:

Стол учительский 2 шт, стул 25 шт, стол 10 шт, парта 8 шт, персональный компьютер 12 шт, монитор 22 шт, 1 ибп, проектор 1 шт, полотно 1 шт, доска меловая 1 шт, коммуникационный стенд, 1 телевизор, металлический шкаф 2 шт, 1 сейф.

# 3.2. Информационное обеспечение обучения

Основные источники:

1. Олифер Н.А, Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы // Учебник для вузов,. – Спб.: Питер, 2021. – 1008 с. 1 экз

2. Яворски П. "Ловушка для багов"ISBN 978-5-4461-1708-6 Автор Яворски П. 2020 информационные технологии 272 шт.

3. Бирюков А А Б59 Информационная безонасность: защита и нанадение. -М.: ДМК Пресс, 2020. - 474 с.: ил

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2020.-272с.:ил.

5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2020.-528с.- (Профессиональное образование)

6. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. Техническая защита информации. Учебник для вузов -5-е изд., перераб. и доп. – М.: - Горячая линия – Телеком, 2020. – 616с:ил.

7.Романов О.А. Организационное обеспечение информационной безопасности: учебник для студентов высш. учеб. заведений –М.: Издательский центр «Академия», 2020. – 192с.

8. Самуйлов К.Е, Шалимов И.А., Васин Н.Н., Василевский В.В, Кулябов Д.С., Королькова А.В. Сети и системы передачи информации: телекоммуникационные сети: Учебник и практикум для вузов / – М.: Издательство Юрайт, 2020. – 363 с.

9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2020. – 178 с.: ил..

10. Коды, шифры, сигналы и тайная передача информации / Фред В. Риксон; пер. с англ. А. Галылина – М.:АСТ: Астрель; Владимир: ВКТ, 2020 – 656 с.:ил.

11. Форензика – компьютерная криминалистика / Николай Федоров – М.: «Onebook.ru», 2020. – 420 с.:ил.

12. Bash и кибербезопасность: атака, защита и анализ из командной строки Linux – СПб.: Питер, 2021 – 288 с.:ил.

Дополнительные источники:

1 Руководство администратора Криптон-замок

2. Руководство администратора ППКОП «Астра»

3. Руководство администратора КТМ-256

4. Учебное пособие Структурированная кабельная система NIKOMAX»

Интернет ресурсы:

1. Электронно-библиотечная система [Электронный ресурс] – режим доступа: http:// www.znanium.com/ (2020).

2. Сайт ФСТЭК РФ [Электронный ресурс] – режим доступа: http://www.fstec.ru

3. [Электронный ресурс] – режим доступа: http://www.ancad.ru сайт компании АНКАД

4. [Электронный ресурс] – режим доступа: https://www.cryptopro.ru/ сайт компании КриптоПро

5. ОАО «ИнфоТеКС» [Электронный ресурс] – режим доступа: https://infotecs.ru/ сайт

6. Центр оказания образовательных услуг и подготовки специалистов в области информационной безопасности и эксплуатации средств защиты информации ViPNet. [Электронный ресурс] – режим доступа: https://edu.infotecs.ru/learning/ (2020)

# 4. Контроль и оценка результатов освоения профессионального модуля (пО РАЗДЕЛАМ)

|  |  |  |
| --- | --- | --- |
| **Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля** | **Критерии оценки** | **Методы оценки** |
| **Раздел модуля 1. Организация защиты информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных 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. | Оценка «**отлично**» - установлены, настроены, испытаны и сконфигурированы программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС;  Оценка «**хорошо**» - установлены, настроены, испытаны программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС;  Оценка «**удовлетворительно**» - установлены, настроены программные и программно-аппаратные (в том числе криптографических) средств защиты информации в оборудовании ИТКС; | Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием  Защита отчетов по практическим и лабораторным работам |
| ПК 2.2 Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. | Оценка «**отлично**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.  Оценка «**хорошо**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях.  Оценка «**удовлетворительно**» - Поддерживать бесперебойную работу программных и программно-аппаратных, в том числе и криптографических средств защиты информации в информационно – телекоммуникационных системах и сетях. | Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием  Защита отчетов по практическим и лабораторным работам  Интерпретация резуль­татов наблюдений за деятельностью обучающегося в процессе практики |
| **Раздел модуля 2. Методы криптографической защиты информации** | | |
| 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. | Оценка «**отлично**» - 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.  Оценка «**хорошо**» - 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.  Оценка «**удовлетворительно**» - 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. | Экзамен/зачет в форме собеседования: практическое задание по построению стенда с техническим заданием  Защита отчетов по практическим и лабораторным работам  Интерпретация резуль­татов наблюдений за деятельностью обучающегося в процессе практики |

Приложение 1

Обязательное

**КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Личностные результаты** | **Содержание урока (тема, тип урока, воспитательные задачи)** | **Способ организации деятельности** | **Продукт деятельности** | **Оценка процесса формирования ЛР** |
| ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты  ЛР 18 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты | Тема:  «Проблемы информационной безопасности» (4 ч.)  Тип урока:  комплексного применения знаний и способов деятельности – деловая игра  Воспитательная задача:  - закрепление и углубление имеющихся навыков и умений;  - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ | Викторина по информационной безопасности и информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИБ | День специалиста ИТ  Выступление и проекты по ИБ студентов, а так же комплексное  закрепление и применение знаний. | - эмоциональное отношение к своей будущей профессии  - умение работать и выполнять требования трудовой дисциплины |

МДК.2.02 Криптографическая защита информации

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Личностные результаты** | **Содержание урока (тема, тип урока, воспитательные задачи)** | **Способ организации деятельности** | **Продукт деятельности** | **Оценка процесса формирования ЛР** |
| ЛР 17 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием программных и программно-аппаратных, в том числе криптографических средств защиты  ЛР 18 Осуществляющий защиту информации в информационно-телекоммуникационных системах и сетях с использованием технических средств защиты | Тема: «Симметричные алгоритмы шифрования» (4 ч.)  Тип урока:  проверки и оценки знаний и способов деятельности  - Урок турнир  Воспитательная задача:  - закрепление и углубление имеющихся навыков и умений;  - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ | Группа распределяются по паром, Каждой паре дают 3 виртуальные машины, побеждает команда, которая быстрее всех взломает и отгадает шифр. Шифр можно найти в файле на виртуальной машине. | «Взломай систему»  Навык дешифрования, знание принципов работы операционных систем | - эмоциональное отношение к своей будущей профессии  - умение работать и выполнять требования трудовой дисциплины |

1. \*Раздел профессионального модуля – часть программы профессионального модуля, которая характеризуется логической завершенностью и направлена на освоение одной или нескольких профессиональных компетенций. Раздел профессионального модуля может состоять из междисциплинарного курса или его части и соответствующих частей учебной и производственной практик. Наименование раздела профессионального модуля должно начинаться с отглагольного существительного и отражать совокупность осваиваемых компетенций, умений и знаний. [↑](#footnote-ref-1)