***Приложение I.3***

***к программе СПО 11.02.15* *«Инфокоммуникационные сети и системы связи»***

**РАБОЧАЯ ПРОГРАММА**

**ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

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

**2022**

**Составитель:**

**Кислицин Никита Алексеевич, преподаватель ГБПОУ УКРТБ**

**Кабирова Эльмира Ринатовна, 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.03. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СЕТЕЙ И СИСТЕМ СВЯЗИ |

*наименование профессионального модуля*

**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 традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.  (в ред. Приказа Минпросвещения России от 17.12.2020 N 747) |
| 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 языках.  (в ред. Приказа Минпросвещения России от 17.12.2020 N 747) |

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 ходе освоения профессионального модуля учитывается движение к достижению личностных результатов обучающимися ЛР 15,17,18.

В результате освоения профессионального модуля студент должен:

|  |  |
| --- | --- |
| Иметь практический опыт в | анализе сетевой инфраструктуры;  выявлении угроз и уязвимости в сетевой инфраструктуре;  разработке комплекса методов и средств защиты информации в инфокоммуникационных сетях и системах связи;  осуществлении текущего администрирования для защиты инфокоммуникационных сетей и систем связи;  использовании специализированного программного обеспечения и оборудования для защиты инфокоммуникационных сетей и систем связи.  *Вариативный практический опыт* |
| уметь | классифицировать угрозы информационной безопасности в инфокоммуникационных системах и сетях связи;  определять оптимальные способы обеспечения информационной безопасности;  осуществлять мероприятия по проведению аттестационных работ и выявлению каналов утечки;  выявлять недостатки систем защиты в системах и сетях связи с использованием специализированных программных продуктов  выполнять расчет и установку специализированного оборудования для обеспечения максимальной защищенности сетевых элементов и логических сетей;  защищать базы данных при помощи специализированных программных продуктов.  *Вариативные умения* |
| знать | принципы построения информационно-коммуникационных сетей;  международные стандарты 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;  классификацию угроз сетевой безопасности;  методы и способы защиты информации, передаваемой по кабельным направляющим системам;  правила проведения возможных проверок согласно нормативным документам Федеральной службы по техническому и экспортному контролю;  средства защиты различных операционных систем и среды передачи информации.  *Вариативные знания* |

**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**

**2.1. Структура профессионального модуля**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Коды профессиональных общих компетенций | Наименования разделов профессионального модуля | Суммарный объем нагрузки, час. | Объем профессионального модуля, час. | | | | | | | | | Самостоятельная работа*[[1]](#footnote-1)* |
| *Обучение по МДК* | | | | | | *Практики* | | |
| Всего | *В том числе* | | | | |
| Лабораторных и практических занятий | | Курсовых работ (проектов) | | | Учебная | Производственная | |
| 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) 8 | | | | | | | | | | | |
|  | **Всего:** | **482** | **282** | | **140** | | **-** | **72** | | **72** | | **28** |

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

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **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.** Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи | | | | | **166** | | |
| **МДК 03.01**  **Технология применения программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи** | | | | | **166** | | |
| **Тема 1.1. Обеспечение безопасности операционных систем** | **Содержание** | | | | **59** | | |
| 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** | | | | 7 | | |
| Подготовить выступление на тему «Уязвимости в операционной системе Windows». | | | |
| **Тема 1.2 Обеспечение безопасности информационных технологий** | **Содержание** | | | | **61** | | |
| 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** | | | | 7 | | |
| **Подготовить выступление на тему «Уязвимости в операционной системе Windows server».** | | | |
| **Тема 1.3. Обеспечение безопасности компьютерных систем и сетей. Технологии Data Leakage Prevention (DLP).** | **Содержание** | | | | **42** | | |
| 1 | Защита информации от внутренних угроз информационной безопасности. Выявление утечек с использованием технологии Data Leakage Prevention (DLP). Теория и практика применения DLP-систем. | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [6] стр. 64-66 | | | | | |
| 2 | Установка, конфигурирование и устранение неисправностей в системе корпоративной защиты от внутренних угроз. | | | 2 | | |
| **Домашнее задание:** составить план конспекта лекции | | |  | | |
| 3 | Установка DLP IWTM в виртуальном окружении. Режимы port mirroring и proxy. | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [6] стр. 66-72 | | |  | | |
| 4 | Конфигурирование DLP IWTM  Исправление типовых неисправностей. | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [6] стр. 72-75 | | |  | | |
| 5 | Технологии агентского мониторинга  Назначение агентского мониторинга. Установка и настройка агентского мониторинга. Интерфейс консоли DLP IWDM. Работа в консоли управления агентом | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |  | | |
| 6 | Политики агентского мониторинга, особенности их настройки. Создание и проверка политик. Создание политик защиты на агентах; Фильтрация событий;  Настройка совместных событий агентского и сетевого мониторинга; Работа с носителями и устройствами; Работа с файлами; Контроль приложений; Исключение из событий перехвата. | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |  | | |
| 7 | Разработка политик безопасности, анализ выявленных инцидентов | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |  | | |
| 8 | Разработка и тестирование политик в системе DLP IWTM. Работа с разделом технологии системы корпоративной защиты: категории и термины, текстовые объекты; Работа с событиями, запросы, объекты перехвата, идентификация контактов в событии; Работа со сводками, виджетами, сводками; Работа с персонами; Работа с объектами защиты; Провести имитацию процесса утечки конфиденциальной информации в системе; Создать непротиворечивые политики, соответствующие нормативной базе и законодательству; Задокументировать созданные политики используя в соответствии с требованиями современных стандартов в области защиты информации. Работа с категориями и терминами; Использование регулярных выражений; Использование морфологического поиска; • Работа с графическими объектами; Работа с выгрузками и баз данных; Работа с печатями и бланками; Работа с файловыми типами; | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |  | | |
| 9 | Мониторинг трафика. Проверка применения политик 4-х видов: трафик, персоны, буфер обмена, движение файлов. Работа с краулером. | | | 2 | | |
| **Домашнее задание:** чтение и анализ литературы [1] стр. 165-172 | | |  | | |
| **Практические занятия** | | | | **24** | | |
| 24-26 | Установка, конфигурирование и  устранение неисправностей в системе  корпоративной защиты от внутренних угроз | | |
| 27-29 | Разработка политик безопасности в  системе корпоративной защиты информации от  внутренних угроз | | |
| 30-32 | Поиск и предотвращение  инцидентов. Технологии анализа сетевого  трафика в системе корпоративной защиты  информации от внутренних угроз | | |
| 33-34 | Технологии агентского мониторинга | | |
| 35 | Анализ выявленных инцидентов | | |
| **Промежуточная аттестация (экзамен)** | | | | | 8 | | |

|  |  |  |
| --- | --- | --- |
| **Раздел 2.**  **Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи** | | **164** |
| **МДК 03.02**  Технология применения комплексной системы защиты информации в инфокоммуникационных системах и сетях связи | | **164** |
| **Тема 2.1.** Основы информационной безопасности | **Содержание** | **33** |
| 1. Основные понятия информационной безопасности. Сущность и понятия защиты информации. Значение информационной безопасности и ее место в системе национальной безопасности. | 20 |
| 2. Виды и источники угроз информационной безопасности Российской Федерации. Доктрина информационной безопасности Российской Федерации. |
| 3. Основные составляющие национальных интересов Российской Федерации в информационной сфере. Конституция РФ и другие основополагающие документы, затрагивающие интересы РФ в информационной сфере. |
| 4. Состояние информационной безопасности РФ и основные задачи по ее обеспечению. Государственная система обеспечения информационной безопасности Российской Федерации. Регуляторы в области информационной безопасности. |
| **Тематика практических занятий и лабораторных работ** | **10** |
| 1. Требования к безопасности информационных систем | 2 |
| 2. Требования к безопасности информационных систем в России | 4 |
| 3. Определение требований к защите информации | 4 |
| **Самостоятельная работа** | **3** |
| 1. Изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере. | 3 |
| **Тема 2.2.** Организационно-правовые аспекты защиты информации | **Содержание** | **44** |
| 1. Структура правовой защиты информации. Система документов в области защиты информации. | 30 |
| 2. Организационные основы защиты информации. Принципы организационной защиты информации. |
| 3. Государственные регуляторы в области защиты информации, их полномочия и сфера компетенции. Обзор стандартов и методических документов в области защиты информации. Регулирующие организации в области защиты информации. |
| 4. Классификация информации по категориям доступа. Критерии оценки информации. Категории нарушений по степени важности. Ответственность за правонарушения в информационной сфере. Руководящие документы, регламентирующие ответственность. Виды ответственности за правонарушения в информационной сфере. |
| **Тематика практических занятий и лабораторных работ** | **10** |
| 1. Правовое регулирование в информационной сфере | 2 |
| 2. Типизация ИСПДН учреждения | 2 |
| 3. Проведение анализа информации на предмет её целостности | 2 |
| 4. Организация и проведение мероприятий по защите ПДн | 4 |
| **Самостоятельная работа** | **4** |
| 1. Подготовка презентации по заданной теме с последующим представлением преподавателю в электронном виде. | 4 |
| **Тема 2.3.**Комплексная система защиты информации | **Содержание** | **45** |
| 1. Общая характеристика комплексной защиты информации. Основы обеспечения комплексной защиты информации. Сущность и задачи комплексной защиты информации. Стратегии комплексной защиты информации. Структура и основные характеристики комплексной защиты информации. | 30 |
| 2. Конфиденциальные сведения. Виды конфиденциальной информации. Персональные данные. Коммерческая тайна. Банковская тайна. |
| 3. Система физической защиты. Обобщенная структурная схема охраны объекта. Посты охраны. Подсистема инженерной защиты. Периметровая сигнализация и ограждение. Периметровое освещение. |
| 4. Способы и средства обнаружения угроз. Комплексное обследование защищенности информационной системы. Средства нейтрализации угроз. |
| **Тематика практических занятий и лабораторных работ** | **12** |
| 1. Исследование уязвимостей и построение модели угроз объекта защиты. | 4 |
| 2. Разработка комплексной системы инженерно-технической защиты информации на объекте. | 4 |
| 3. Исследование возможностей устройства для защиты объектов информатизации | 4 |
| **Самостоятельная работа** | **3** |
| 1. Составление доклада по перспективе и направлению развития комплексных средств защиты информации на основе публикаций в периодической литературе. | 3 |
| **Тема 2.4.** Инженерно-техническая защита информации | **Содержание** | **68** |
| 1. Основы инженерно-технической защиты информации. Подразделения технической защиты информации и их основные задачи. Механические системы защиты. | 44 |
| 2. Понятие несанкционированного доступа к защищаемой информации. Понятие НСД к информации. Виды НСД к информации. Основные способы и средства НСД к защищаемой информации. Активные способы НСД к информации. |
| 3. Технические каналы утечки информации. Общая структура канала утечки информации. Классификация каналов утечки информации. Защита информации от утечки по техническим каналам передачи информации. Пассивное противодействие НСД. |
| 4. Обеспечение безопасности телефонных переговоров. Противодействие незаконному подключению к линиям связи. Противодействие контактному и бесконтактному подключению. Защита от перехвата. Противодействие несанкционированному доступу к источникам конфиденциальной информации. Защита информации в каналах связи. Акустический контроль. Понятие разборчивости речи при перехвате информации. Способы и средства информационного скрытия речевой информации от подслушивания. |
| 5. Демаскирующие признаки закладных устройств. Классификация средств обнаружения и локализации закладных устройств и их излучений. Классификация средств обнаружения неизлучающих закладок. Контроль линий связи, отходящих от технических средств. Принципы контроля телефонных линий и цепей электропитания и заземления. Принципы контроля цепей электропитания. Контроль слаботочных цепей. Принципы контроля линий заземления. |
| 6. Средства нелинейной радиолокации. Принципы работы устройств нелинейной радиолокации. Нелинейные радиолокаторы. Современные средства радиолокации. Методы поиска радиоизлучений закладных устройств. Индикаторы поля. Обнаружение радиоизлучений. Панорамные радиоприемники. Сканирующие приемники. |
| **Тематика практических занятий и лабораторных работ** | **20** |
| 1. Анализ источников, каналов распространения и каналов утечки информации | 2 |
| 2. Анализ методов и средств физических защиты информации и их классификации | 2 |
| 3. Составление инструкции по обработке и хранению конфиденциальной документов | 2 |
| 4. Анализ источников, каналов распространения и каналов утечки информации | 4 |
| 5. Исследование возможностей системы оценки защищенности выделенных помещений | 2 |
| 6. Изучение методов построения КСЗИ сетевых приложений и баз данных | 4 |
| 7. Классификация автоматизированных систем обработки информации по классу защиты информации | 2 |
| 8. Оценка безопасности информации на объектах её обработки | 2 |
| **Самостоятельная работа** | **4** |
| 1. Разработка предложений по инженерно-технической защите информации на определенном объекте. | 4 |
| **Тема 2.5.**Криптографическая защита информации | **Содержание** | **36** |
| 1. Основы криптографии. Структура криптосистемы. Основные методы криптографического преобразования данных. | 26 |
| 2. Симметричные криптосистемы. Шифрование методом замены. Шифрование методом перестановки. Шифрование методом гаммирования. Криптосистемы с открытым ключом. Основы шифрования с открытым ключом. Алгоритм обмена ключами Диффи-Хеллмана. Алгоритм шифрования Rivest-Shamir-Adleman (RSA) с открытым ключом. |
| 3. Системы электронной подписи. Проблема аутентификации данных и электронная цифровая подпись. Технология работы электронной подписи. Безопасные хеш-функции, алгоритмы хеширования. Контрольное значение циклического избыточного кода CRC. Цифровые сертификаты. Отечественный стандарт цифровой подписи. Понятие криптоанализа. |
| **Тематика практических занятий и лабораторных работ** | **10** |
| 1. Поиск и локализация скрытых видеокамер | 4 |
| 2. Применение методов шифрования перестановкой | 4 |
| 3. Создание скрытой информации. Установка паролей. | 2 |
| **Тема 2.6.**Аттестация и лицензирование объектов защиты | **Содержание** | **22** |
| 1. Общие вопросы по аттестации ОИ по требованиям безопасности информации. Основные стадии создания системы защиты информации на ОИ. Порядок проведения аттестации объектов информатизации. Организационная структура системы аттестации объектов информатизации. Программа и методика проведения аттестационных испытаний. | 14 |
| 2. Лицензирование деятельности в области защиты конфиденциальной информации. Документы, разрабатываемые на объектах информатизации. Документы, разрабатываемые на аттестуемое помещение. Порядок действий при лицензировании. |
| **Тематика практических занятий и лабораторных работ** | **8** |
| 1. Обнаружение, идентификация и локализация цифровых радиопередающих устройств с помощью индикаторов поля | 4 |
| 2. Поиск и обнаружение радиоизлучающих средств | 4 |
| **Промежуточная аттестация (экзамен)** | | **10** |
| **Самостоятельная работа при изучении раздела 2 ПМ 03:**  - изучение основополагающих документов, затрагивающих интересы РФ в информационной сфере;  - ознакомление с нормативными документами по ИБ;  - изучение специализированной литературы, периодической печати по вопросам оказания новых услуг в сфере информационной безопасности;  - составление доклада по перспективным направлениям развития средств комплексной защиты информации;  - разработка пакета документации по инженерно-технической защите информации на объекте;  - изучение возможностей инженерно-технических средств защиты информации;  - изучение технических характеристик инженерно-технических средств защиты информации;  - разработка предложений по инженерно-технической защите информации на определенном объекте; | | **14** |
| **Учебная практика(по профилю специальности) по ПМ 03**  **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. | | **72** |
| **Производственная практика (по профилю специальности) по ПМ**  **Виды работ:**  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. | | **72** |
| **Промежуточная аттестация (экзамен)** | | **8** |
| **Всего** | | **482** |

# **3. условия реализации программы ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

# **3.1. Требования к минимальному материально-техническому обеспечению**

Реализация программы модуля предполагает наличие Лаборатория телекоммуникационных систем, лаборатория сетей абонентского доступа, Лаборатория основ телекоммуникаций.

Стол учительский 2 шт, парты ученические 6 шт, доска 1 шт, доска флипчарт 1 шт, проектор 1 шт, стол компьютерный 11 шт, шкаф 1 шт, стенд 9 шт, стойка 3 шт, персональный компьютер 13 шт, двухрамная стойка 1 шт, учебная установка «Изучение принципов временного разделения каналов» 2 шт.; учебная установка «Изучение ИКМ кодека» 2 шт; учебная установка «Изучение приемника и передатчика DTMF сигналов» 2 шт; учебная установка «Изучение электронных телефонных аппаратов» 2 шт; учебная лабораторная установка «Исследование мобильных телефонов» 2 шт; учебная лабораторная установка «Сенсорные сети ZigBee» 2 шт; учебная лабораторная установка «Изучение GPS-приемников» 2 шт; учебная лабораторная установка «Персональные сети Bluetooth» 2 шт; аппаратно-программный комплекс «Изучение принципов построения и исследование технологий инфокоммуникационных сетей» 2 шт; аппаратно-программный комплекс «Изучение принципов построения и исследование технологий глобальных IP-сетей» 2 шт, учебно-лабораторный комплекс, «Корпоративные сети».

Лаборатория информационной безопасности телекоммуникационных систем:

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. Фороузан Б.А. Криптография и безопасность сетей: Учебное пособие/ Фороузан Б.А.; пер. с англ. Под ред.А.Н. Берлина. - М.: Интернет-Университет Информационных технологий: БИНОМ. Лаборатория знаний, 2020.-784с.:ил.,табл.-(Основы информационных технологий).2. Максименко В.Н., Афанасьев В.В., Волков Н.В. Защита информации в сетях сотовой подвижной связи/ Под ред. доктора техн. Наук, профессора О.Б. Макаревича. – М.: Горячая линия – Телеком, 2019. -360с.: ил.

3. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства –М.: ДМК Пресс, 2016. – 544с.:ил.

4. Родичев Ю.А. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. –СПб.:2021.-272с.:ил.

5. Васильков А.В., Васильков А.А., Васильков И.А Информационные системы и их безопасность: учебное пособие –М.: ФОРУМ, 2019.-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, 2021. – 363 с.

9. InfoWatch Traffic Monitor Руководство пользователя – М.: ЗАО "ИнфоВотч", 2022. – 178 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/ (2022).

2. http://www.fstec.ru сайт ФСТЭК РФ

3. http://www.ancad.ru сайт компании АНКАД

4. https://www.cryptopro.ru/ сайт компании КриптоПро

5. https://infotecs.ru/ сайт ОАО «ИнфоТеКС»

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/ (2022)

# **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 1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи** | | |
| ПК 3.1. Выявлять угрозы и уязвимости в сетевой инфраструктуре с использованием системы анализа защищенности | Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.  Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.  Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию. | тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
| ПК 3.3. Осуществлять текущее администрирование для защиты инфокоммуникационных сетей и систем связи с использованием специализированного программного обеспечения и оборудования. |
| **Раздел 2.**  **Применение комплексной системы защиты информации в инфокоммуникационных системах и сетях связи** | | |
| ПК 3.2. Разрабатывать комплекс методов и средств защиты информации в инфокоммуникационных сетях и системах связи. | Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.  Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.  Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию. | тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
| тестирование,  экзамен,  экспертное наблюдение выполнения лабораторных работ,  экспертное наблюдение выполнения практических работ,  оценка решения ситуационных задач,  оценка процесса и результатов выполнения видов работ на практике |
|  | | |

|  |  |  |
| --- | --- | --- |
| ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам. | * обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач;   - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы  Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам  Экзамен |
| ОК 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности. | - использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач |
| ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие. | - демонстрация ответственности за принятые решения  - обоснованность самоанализа и коррекция результатов собственной работы; |
| ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. | - взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик;  - обоснованность анализа работы членов команды (подчиненных) |
| ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. | -грамотность устной и письменной речи,  - ясность формулирования и изложения мыслей |
| ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.  (в ред. Приказа Минпросвещения России от 17.12.2020 N 747) | - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, |
| ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик;  - знание и использование ресурсосберегающих технологий в области телекоммуникаций |
| ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. | - эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; |
| ОК 09. Использовать информационные технологии в профессиональной деятельности. | - эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту; |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках.  (в ред. Приказа Минпросвещения России от 17.12.2020 N 747) | - эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке. |

Приложение 1

Обязательное

**КОНКРЕТИЗАЦИЯ ДОСТИЖЕНИЯ ЛИЧНОСТНЫХ РЕЗУЛЬТАТОВ**

МДК.3.1 Применение программно-аппаратных средств защиты информации в инфокоммуникационных системах и сетях связи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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  День специалиста ИТ (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 информационным технологиям с использование электронных средств и проектов. Состоит из 2 частей, теоретическая игра Quiz и защита проектов по ИТ | Выступление и проекты по ИТ студентов, а так же комплексное  закрепление и применение знаний. | - эмоциональное отношение к своей будущей профессии  - умение работать и выполнять требования трудовой дисциплины |

МДК 03.02 Технология применения комплексной системы защиты информации в

инфокоммуникационных системах и сетях связи

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Личностные результаты** | **Содержание урока (тема, тип урока, воспитательные задачи)** | **Способ организации деятельности** | **Продукт деятельности** | **Оценка процесса формирования ЛР** |
| ЛР 15. Осознающий важность соблюдения норм законодательства и внутренней документации в отношении использования и сохранности конфиденциальной и инсайдерской информации, полученной в результате исполнения своих должностных обязанностей  ЛР 18. Обеспечивающий информационную безопасность инфокоммуникационных сетей и систем связи | **Тема: Инженерно-техническая защита информации** (68 ч)  **Тип урока:** проверки и оценки знаний и способов деятельности  **Воспитательная задача:**  - формирование уважения к своей будущей профессии  - формирование представления о возможности карьерного роста при условии непрерывного образования  - развитие ответственного отношения к организации и ходу продуктивной деятельности при выполнении проектных работ | Участие всей группы.  Студентам во время начала урока объясняются правила проведения игры, затем выдаётся ссылка или QR код для доступа к игре.  Последовательно отвечая на вопросы в конце игры автоматически объявляются победители. | «Аукцион знаний»  Игра на платформе LearningApp.org | - навыки анализа и интерпретации информации из различных источников  - стремление к повышению профессионального уровня  - эмоциональное отношение к своей будущей профессии  - уровень мотивации проявления стремления работать по своей специальности |

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. [↑](#footnote-ref-1)