**Санкт-Петербургское государственное бюджетное**
**профессиональное образовательное учреждение**
**«Колледж автоматизации производственных процессов**
**и прикладных информационных систем»**

Рассмотрена и принята
Педагогическим советом
Протокол № 12 от 15.06.2023

УТВЕРЖДЕНА
Приказом
СПб ГБПОУ «Колледж автоматизации производства»
от 10.07.2023 №479

# РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Для специальности **09.02.06 Сетевое и системное администрирование**

Санкт-Петербург

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) по специальности 09.02.06 «Сетевое и системное администрирование», утвержденного приказом Министерства образования и науки РФ от 9 декабря 2016 г. № 1548.

Организация-разработчик: Санкт-Петербургское государственное бюджетное профессиональное образовательное учреждение «Колледж автоматизации производственных процессов и прикладных информационных систем»

Программу составили: Николаенко А.И., Казакова Н.В., Баранаускас Д.К., преподаватель Санкт-Петербургского государственного бюджетного профессионального образовательного учреждения «Колледж автоматизации производственных процессов и прикладных информационных систем».

Программа рассмотрена и одобрена на заседании методической комиссии, протокол № 8 от 11.05.2023.

Заведующий отделом СОП А.Ф. Жмайло

## 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПМ.03
## «Эксплуатация объектов сетевой инфраструктуры»

### 1.1. Область применения программы

Рабочая программа профессионального модуля (далее рабочая программа) – является вариативной частью ППССЗ в части освоения основного вида профессиональной деятельности (ВПД): «Эксплуатация объектов сетевой инфраструктуры» и соответствующих профессиональных компетенций.

### 1.2. Цели и задачи модуля – требования к результатам освоения модуля

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями учащийся в ходе освоения профессионального модуля должен:

**иметь практический опыт в:**

- обслуживании сетевой инфраструктуры, восстановлении работоспособности сети после сбоя;
- удаленном администрировании и восстановлении работоспособности сетевой инфраструктуры;
- поддержке пользователей сети, настройке аппаратного и программного обеспечения сетевой инфраструктуры.

**уметь:**

- выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;
- осуществлять диагностику и поиск неисправностей всех компонентов сети;
- выполнять действия по устранению неисправностей
- *устанавливать системы обнаружения и предотвращения вторжений;*
- *работать с системой обнаружения и предотвращения вторжений;*
- *создавать защищённую сеть;*
- *настраивать и модифицировать межсетевое взаимодействие;*
- *устанавливать DLP-систему;*
- *создавать правила и политики безопасности в DLP-системах;*
- *создавать отчёты по инцидентам в DLP-системах;*
- *применять на практике алгоритмы шифрования секретным ключом;*
- *проводить анализ криптостойкости алгоритмов и протоколов;*
- *создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;*
- *конструировать крипто-стойкие алгоритмы и протоколы;*
- *проводить анализ данных на наличие скрытой информации*

**знать:**

- архитектуру и функции систем управления сетями, стандарты систем управления;
- средства мониторинга и анализа локальных сетей;
- методы устранения неисправностей в технических средствах;
- *системы обнаружения вторжения;*
- *программно-аппаратные средства для создания защищённой сети;*
- *DLP-системы для защиты от внутренних утечек информации*

- *основные понятия, определения, основные алгоритмы шифрования с секретным ключом;*
- *основные понятия, определения, модель передачи защищенных сообщений с открытым ключом шифрования;*
- *основные понятия, определения и алгоритмы стеганографии;*
- *основные принципы анализа криптографических систем.*

### 1.3. Планируемое количество часов на освоение программы ПМ.03

| № | Вид учебной работы | Объем часов |
|---|---|---|
| **1.** | **Объем работы обучающихся во взаимодействии с преподавателем** | **912** |
| в том числе: | | |
| теоретическое обучение | | 194 |
| практические занятия | | 304 |
| учебная практика | | 72 |
| производственная практика | | 324 |
| **Промежуточная аттестация в форме экзамена** | | **18** |
| **2.** | **Самостоятельная внеаудиторная работа обучающихся** | **56** |
| **Всего по ПМ.03 в рамках образовательной программы** | | **960** |

## 2. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ ПМ.03

Результатом освоения программы профессионального модуля является овладение обучающимися видом профессиональной деятельности «Выполнение работ по проектированию сетевой инфраструктуры», в том числе профессиональными (ПК) и общими (ОК) компетенциями.

| Код | Наименование результата обучения |
|---|---|
| ПК 3.1 | Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей. |
| ПК 3.2 | Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях. |
| ПК 3.3. | Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации. |
| ПК 3.4. | Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации. |
| ПК 3.5. | Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта. |
| ПК 3.6. | Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры. |
| *ПК.3.7* | *Применять программно-аппаратные средства защиты информации на защищаемых объектах* |
| *ПК 3.8* | *Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов* |
| *ПК3.9* | *Применять криптографические аппаратные средства защиты информации на защищаемых объектах* |
| ОК 1. | Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам |
| ОК 2. | Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности |
| ОК 3. | Планировать и реализовывать собственное профессиональное и личностное развитие. |
| ОК 4. | Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами. |
| ОК 5. | Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста. |
| ОК 6. | Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. |
| ОК 7. | Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. |
| ОК 8. | Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности. |
| ОК 9. | Использовать информационные технологии в профессиональной деятельности |
| ОК 10. | Пользоваться профессиональной документацией на государственном и иностранном языке. |

| | |
|---|---|
| ОК 11. | Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере |

## 3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

### 3.1. Тематический план профессионального модуля

| Коды профессиональных компетенций | Наименования разделов профессионального модуля | Всего часов *(макс. учебная нагрузка и практики)* | Объем времени, отведенный на освоение междисциплинарного курса (курсов) | | | | | Практика | |
|---|---|---|---|---|---|---|---|---|---|
| | | | Обязательная аудиторная учебная нагрузка обучающегося | | | Самостоятельная работа обучающегося | | Учебная, часов | Производственная (по профилю специальности), часов |
| | | | Всего, часов | в т.ч. лабораторные работы и практические занятия, часов | в т.ч., курсовая работа (проект), часов | Всего, Часов | в т.ч., курсовая работа (проект), часов | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| ПК 3.1 – ПК 3.6. | Раздел 1. Эксплуатация объектов сетевой инфраструктуры | 174 | 156 | 90 | | 18 | | | |
| ПК 3.1 – ПК 3.6. | Раздел 2. Безопасность компьютерных сетей | 198 | 188 | 90 | | 10 | | | |
| ПК 3.7. - ПК 3.8. | Раздел 3.Защита от внутренних угроз информационной безопасности | 88 | 78 | 72 | 20 | 10 | 20 | | |
| ПК 3.9 | Раздел 4.Основы криптографической защиты данных | 68 | 64 | 50 | | 4 | | | |
| ПК 3.1 – ПК 3.9. | Учебная практика, производственная практика (по профилю специальности), часов | 360 | | | | | | 72 | 288 |
| ПК 3.1 – ПК 3.9. | Промежуточная аттестация по ПМ.03 | 18 | | | | | | | |
| | Всего: | 906 | 486 | 304 | 20 | 42 | 20 | 72 | 288 |

**3.2. Содержание обучения по профессиональному модулю (ПМ)**

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| **Раздел 1. Эксплуатация объектов сетевой инфраструктуры** | | **174** |
| **Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры** | **Содержание учебного материала** | **18** |
| | 1.1.1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки. Полоса пропускания, паразитная нагрузка. | 2 |
| | 1.1.2. Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб). Наращивание длины сегментов сети; замена существующей аппаратуры. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети. | 2 |
| | 1.1.3. Техническая и проектная документация. Паспорт технических устройств. Физическая карта всей сети; логическая топология компьютерной сети. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. | 2 |
| | 1.1.4. Проверка объектов сетевой инфраструктуры и профилактические работы | 2 |
| | 1.1.5. Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках. | 2 |
| | 1.1.6. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. | 2 |
| | 1.1.7. Протокол SNMP, его характеристики, формат сообщений, набор услуг. | 2 |
| | 1.1.8. Задачи управления: анализ производительности и надежности сети. | 2 |
| | 1.1.9. Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры. | 2 |
| | **Практические занятия** | **40** |
| | **Практическое занятие № 1** Оконцовка кабеля витая пара | 2 |
| | **Практическое занятие № 2** Заделка кабеля витая пара в розетку | 2 |
| | **Практическое занятие № 3** Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену | 2 |
| | **Практическое занятие № 4** Тестирование кабеля | 2 |
| | **Практическое занятие № 5** Поддержка пользователей сети. | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | **Практическое занятие № 6** Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы) | 2 |
| | **Практическое занятие № 7** Выполнение действий по устранению неисправностей | 2 |
| | **Практическое занятие № 8** Выполнение мониторинга и анализа работы локальной сети с помощью программных средств. | 2 |
| | **Практическое занятие № 9** Оформление технической документации, правила оформления документов | 2 |
| | **Практическое занятие № 10** Протокол управления SNMP | 2 |
| | **Практическое занятие № 11** Основные характеристики протокола SNMP | 2 |
| | **Практическое занятие № 12** Набор услуг (PDU) протокола SNMP | 2 |
| | **Практическое занятие № 13** Формат сообщений SNMP | 2 |
| | **Практическое занятие № 14** Задачи управления: анализ производительности сети | 2 |
| | **Практическое занятие № 15** Задачи управления: анализ надежности сети | 2 |
| | **Практическое занятие № 16** Управление безопасностью в сети. | 2 |
| | **Практическое занятие № 17** Учет трафика в сети | 2 |
| | **Практическое занятие № 18** Средства мониторинга компьютерных сетей | 2 |
| | **Практическое занятие № 19** Средства анализа сети с помощью команд сетевой операционной системы | 2 |
| | **Практическое занятие № 20** Эксплуатация объектов сетевой инфраструктуры | 2 |
| **Тема 1.2. Эксплуатация систем IP-телефонии** | **Содержание учебного материала** | **34** |
| | 1.2.1. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323. | 2 |
| | 1.2.2. Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. | 2 |
| | 1.2.3. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. | 2 |
| | 1.2.4. Обеспечение отказоустойчивости. | 2 |
| | 1.2.5. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. | 2 |
| | 1.2.6. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. | 2 |
| | 1.2.7. Модель установления соединения. Планирование отказоустойчивости. | 2 |
| | 1.2.8. Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры ин- | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | стalляции. | |
| | 1.2.9. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация. | 2 |
| | 1.2.10. Управление программным коммутатором. Маршрутизация. Группы соединительных линий. | 2 |
| | 1.2.11. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. | 2 |
| | 1.2.12. Группы абонентов. Дополнительные абонентские услуги. | 2 |
| | 1.2.13. Организация эксплуатации систем IP-телефонии. | 2 |
| | 1.2.14. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт. | 2 |
| | 1.2.15. Техническая и проектная документация, способы резервного копирования данных, принцип работы хранилищ данных | 2 |
| | 1.2.16. Восстановление работы сети после аварии. | 2 |
| | 1.2.17. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных | 2 |
| | **Практические занятия** | **40** |
| | **Практическое занятие № 21**Настройка аппаратных IP-телефонов | 2 |
| | **Практическое занятие № 22** Настройка программных IP-телефонов, факсов | 2 |
| | **Практическое занятие № 23** Развертывание сети с использованием VLAN для IP-телефонии | 2 |
| | **Практическое занятие № 24** Настройка шлюза | 2 |
| | **Практическое занятие № 25** Установка, подключение и первоначальные настройки голосового маршрутизатора | 2 |
| | **Практическое занятие № 26** Настройка таблицы пользователей в голосовом маршрутизаторе | 2 |
| | **Практическое занятие № 27** Настройка групп в голосовом маршрутизаторе | 2 |
| | **Практическое занятие № 28** Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе | 2 |
| | **Практическое занятие № 29** Настройка голосовых сообщений в маршрутизаторе | 2 |
| | **Практическое занятие № 30** Настройка программно-аппаратной IP-АТС | 2 |
| | **Практическое занятие № 31** Установка и настройка программной IP-АТС | 2 |
| | **Практическое занятие № 32** Тестирование кодеков. Исследование параметров качества обслужива- | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | ния | |
| | **Практическое занятие № 33** Мониторинг и анализ соединений по различным протоколам | 2 |
| | **Практическое занятие № 34** Мониторинг вызовов в программном коммутаторе | 2 |
| | **Практическое занятие № 35** Создание резервных копий баз данных | 2 |
| | **Практическое занятие № 36** Диагностика и устранение неисправностей в системах IP-телефонии | 2 |
| | **Практическое занятие № 37** Эксплуатация систем IP-телефонии | 2 |
| | **Практическое занятие № 38** Восстановление работы сети после аварии | 2 |
| | **Практическое занятие № 39** Схемы послеаварийного восстановления работоспособности сети IP-телефонии | 2 |
| | **Практическое занятие № 40** Способы резервного копирования | 2 |
| **Тема 1.3. Инвентаризация технических средств сетевой инфраструктуры , замена расходных материалов и мелкий ремонт периферийного оборудования** | **Содержание учебного материала** | **14** |
| | 1.3.1. Системы инвентаризации сетевых ресурсов | 2 |
| | 1.3.2. Обзор программ для инвентаризации сетей | 2 |
| | 1.3.3. Аудит сетевой инфраструктуры | 2 |
| | 1.3.4. Аудит беспроводной сети | 2 |
| | 1.3.5. Этапы проведения аудита | 2 |
| | 1.3.6. Структура отчета аудита | 2 |
| | Устный зачет по темам 1.1-1.3 | 2 |
| | **Практические занятия** | **10** |
| | **Практическое занятие № 41** Обследование и модернизация сетевой инфраструктуры | 2 |
| | **Практическое занятие № 42** Замена расходных материалов и мелкий ремонт периферийного оборудования | 2 |
| | **Практическое занятие № 43** Составление отчета аудита | 2 |
| | **Практическое занятие № 44** Комплексная работа по эксплуатации систем IP-телефонии | 4 |
| **Самостоятельная работа** | | |
| Заполнение рабочей тетради для самостоятельных работ по МДК.03.01 | | 18 |
| **Экзамен** | | **6** |
| **Раздел 2. Безопасность компьютерных сетей** | | **198** |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| **Тема 2.1. Безопасность компьютерных сетей** | **Содержание учебного материала** | **98** |
| | 2.1.1. Фундаментальные принципы безопасной сети | 2 |
| | 2.1.2. Современные угрозы сетевой безопасности. | 2 |
| | 2.1.3. Вирусы, черви и троянские кони. | 2 |
| | 2.1.4. Методы атак. | 2 |
| | 2.1.5. Безопасность Сетевых устройств OSI | 2 |
| | 2.1.6. Безопасный доступ к устройствам. | 2 |
| | 2.1.7. Назначение административных ролей. | 2 |
| | 2.1.8. Мониторинг и управление устройствами. | 2 |
| | 2.1.9. Использование функция автоматизированной настройки безопасности. | 2 |
| | 2.1.10. Авторизация, аутентификация и учет доступа (AAA) | 2 |
| | 2.1.11. Свойства AAA. | 2 |
| | 2.1.12. Локальная AAA аутентификация. | 2 |
| | 2.1.13. Server-based AAA | 2 |
| | 2.1.14. Реализация технологий брандмауэра | 2 |
| | 2.1.15. ACL. Технология брандмауэра | 2 |
| | 2.1.16. Контекстный контроль доступа (CBAC). | 2 |
| | 2.1.17. Политики брандмауэра основанные на зонах. | 2 |
| | 2.1.18. Реализация технологий предотвращения вторжения | 2 |
| | 2.1.19. IPS технологии. | 2 |
| | 2.1.20. IPS сигнатуры. | 2 |
| | 2.1.21. Реализация IPS. | 2 |
| | 2.1.22. Проверка и мониторинг IPS | 2 |
| | 2.1.23. Безопасность локальной сети | 2 |
| | 2.1.24. Обеспечение безопасности пользовательских компьютеров. | 2 |
| | 2.1.25. Соображения по безопасности второго уровня (Layer-2). | 2 |
| | 2.1.26. Конфигурация безопасности второго уровня. | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | 2.1.27. Безопасность беспроводных сетей, VoIP и SAN | 2 |
| | 2.1.28. Криптографические системы | 2 |
| | 2.1.29. Реализация технологий VPN | 2 |
| | 2.1.30. GRE VPN. | 2 |
| | 2.1.31. Компоненты и функционирование IPSec VPN. | 2 |
| | 2.1.32. Реализация Site-to-site IPSec VPN с использованием CLI. | 2 |
| | 2.1.33. Реализация Site-to-site IPSec VPN с использованием CCP. | 2 |
| | 2.1.34. Реализация Remote-access VPN | 2 |
| | 2.1.35. Управление безопасной сетью | 2 |
| | 2.1.36. Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность | 2 |
| | 2.1.37. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций | 2 |
| | 2.1.38. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности. | 2 |
| | 2.1.39. Cisco ASA. Введение в Адаптивное устройство безопасности ASA. | 2 |
| | 2.1.40. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. | 2 |
| | 2.1.41. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM. | 2 |
| | 2.1.42. Создание удостоверяющего центра на базе ПАК «Крипто ПРО УЦ» | 2 |
| | 2.1.43. Использование Microsoft System Center для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности | 2 |
| | 2.1.44. Применение криптопровайдера VipNet CSP в стандартных приложениях | 2 |
| | 2.1.45. Использование системы Zabbix для мониторинга информационной инфраструктуры и реагирования на инциденты безопасности | 2 |
| | 2.1.46. Классы атак в сетях на основе TCP/IP. Атаки на сетевом и транспортном уровне: Ping, flood, IP spoofing, пассивное сканирование. MITM атаки. Способы предотвращение атак. | 2 |
| | 2.1.47. DOS и DDOS атаки. Атаки отказа в обслуживании DDOS. Виды DDOS атак. Предотвращение DDOS атак. | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | 2.1.48. Обеспечение безопасности канального уровня. MITM атаки канального уровня: ARP-spoofing, DHCP-spoofing, VLAN-hopping, MAC-flooding, атаки на протокол STP. Способы предотвращения атак на канальном уровне. | 2 |
| | 2.1.49. Протоколы SSL/TLS. Основные понятия протоколов SSL и TLS. Устройство, принцип работы протокола SSL.mЦифровые сертификаты. Аутентификация и обмен ключами. | 2 |
| | **Практические занятия** | **90** |
| | **Практическое занятие № 1** Социальная инженерия | 2 |
| | **Практическое занятие № 2** Исследование сетевых атак и инструментов проверки защиты сети | 2 |
| | **Практическое занятие № 3** Безопасность ресурсов и контроль доступа | 2 |
| | **Практическое занятие № 4** Сканирование уязвимостей | 2 |
| | **Практическое занятие № 5** Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам. | 2 |
| | **Практическое занятие № 6** Основные этапы допуска к ресурсам вычислительной системы. | 2 |
| | **Практическое занятие № 7** Допуск к ресурсам сети | 2 |
| | **Практическое занятие № 8** Допуск к ресурсам сервера, базы данных | 2 |
| | **Практическое занятие № 9** Использование динамически изменяющегося пароля. | 2 |
| | **Практическое занятие № 10** Взаимная проверка подлинности и другие случаи опознания. | 2 |
| | **Практическое занятие № 11** Применение различных способов разграничения доступа к компьютерным ресурсам. | 2 |
| | **Практическое занятие № 12** Разграничение доступа по спискам. | 2 |
| | **Практическое занятие № 13** Использование матрицы установления полномочий. | 2 |
| | **Практическое занятие № 14** Произвольное и принудительное управление доступом. | 2 |
| | **Практическое занятие № 15** Настройка безопасного доступа к маршрутизатору | 2 |
| | **Практическое занятие № 16** Обеспечение административного доступа AAA и сервера Radius | 2 |
| | **Практическое занятие № 17** Настройка политики безопасности брандмауэров | 2 |
| | **Практическое занятие № 18** Настройка системы предотвращения вторжений (IPS) | 2 |
| | **Практическое занятие № 19** Настройка безопасности на втором уровне на коммутаторах | 2 |
| | **Практическое занятие № 20** Исследование методов шифрования | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | **Практическое занятие № 21** Автоматическое шифрование логических дисков ПК. | 2 |
| | **Практическое занятие № 22** Настройка Site-to-Site VPN используя интерфейс командной строки | 2 |
| | **Практическое занятие № 23** Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки | 2 |
| | **Практическое занятие № 24** Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM | 2 |
| | **Практическое занятие № 25** Базовая настройка шлюза безопасности ASA и настройка NAT | 2 |
| | **Практическое занятие № 26** Базовая настройка шлюза безопасности ASA и фильтрация трафика с помощью Access Lists | 2 |
| | **Практическое занятие № 27** Маршрутизация в шлюзе безопасности ASA | 2 |
| | **Практическое занятие № 28** Создание правил Modular Policy Framework (MPF) в шлюзе безопасности ASA | 2 |
| | **Практическое занятие № 29** TCP Advanced Options в шлюзе безопасности ASA | 2 |
| | **Практическое занятие № 30** Анализи внутрипротокольного трафика шлюза безопасности ASA | 2 |
| | **Практическое занятие № 31** Работа с логическими интерфейсами шлюза безопасности ASA | 2 |
| | **Практическое занятие № 32** Монитор вторжений **Threat Detection** шлюза безопасности ASA | 2 |
| | **Практическое занятие № 33** Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM | 2 |
| | **Практическое занятие № 34** Перенаправления трафика из шлюза безопасности ASA в Firepower | 2 |
| | **Практическое занятие № 35** Расшифровка трафика в шлюзе безопасности ASA при помощи SSL Decryption | 2 |
| | **Практическое занятие № 36** Сбор статистики о трафике, проходящем через шлюз безопасности ASA | 2 |
| | **Практическое занятие № 37** Автопереключение между двумя провайдерами при помощи шлюза безопасности ASA | 2 |
| | **Практическое занятие № 38** Установка Cisco Identity Services Engine (ISE). | 2 |
| | **Практическое занятие № 39** Cisco ISE добавление Secondary Node | 2 |
| | **Практическое занятие № 40** Установка и настройка SSL VPN | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | **Практическое занятие № 41** Установка и настройка IPSec VPN | 2 |
| | **Практическое занятие № 42** Подключение Cisco ASA и Cisco Router через IPSec VPN | 2 |
| | **Практическое занятие № 43** Настройка Clientless Remote Access SSL VPNs используя ASDM | 2 |
| | **Практическое занятие № 44** Настройка AnyConnect Remote Access SSL VPN используя ASDM | 2 |
| | **Практическое занятие № 45** Обеспечение информационной безопасности | 2 |
| **Самостоятельная работа** | | |
| Заполнение рабочей тетради для самостоятельных работ по МДК.03.02 | | **10** |
| **Дифференцированный зачет** | | **6** |
| | **Раздел 3. Защита от внутренних угроз информационной безопасности** | **156** |
| **Тема 3.1. Системы обнаружения вторжения** | **Содержание учебного материала** | **2** |
| | 3.1.1. Использование систем обнаружения вторжения | 2 |
| | **Практические занятия** | **22** |
| | **Практическое занятие № 1** Установка системы обнаружения и предотвращения вторжения Snort | 2 |
| | **Практическое занятие № 2** Настройка системы обнаружения и предотвращения вторжения Snort | 2 |
| | **Практическое занятие № 3** Установка MySQL для работы со Snort | 2 |
| | **Практическое занятие № 4** Запись предупреждений о вторжениях в MySQL | 2 |
| | **Практическое занятие № 5** Установка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort | 2 |
| | **Практическое занятие № 6** Настройка веб-интерфейса для системы обнаружения и предотвращения вторжения Snort | 2 |
| | **Практическое занятие № 7** Использование стандартных правил для Snort | 2 |
| | **Практическое занятие № 8** Создание собственных правил для Snort. Синтаксис правил | 2 |
| | **Практическое занятие № 9** Настройка виртуальной машины для эмуляции угроз ИБ | 2 |
| | **Практическое занятие № 10** Отслеживание действий в сети и создание своих правил | 2 |
| | **Практическое занятие № 11** Составить сравнительную характеристику средств защиты информации | 2 |
| **Тема 3.2. Использование** | **Содержание учебного материала** | **2** |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| **программно-аппаратных средств для создания защищённой сети** | 3.2.1. Общая характеристика продуктов ViPNet для создания защищённой сети. Понятие построения виртуальной защищённой сети, межсетевой взаимодействие защищённых сетей | 2 |
| | **Практические занятия** | **26** |
| | **Практическое занятие № 12** Развёртывание защищённой сети ViPNet: установка ЦУС | 2 |
| | **Практическое занятие № 13** Развёртывание защищённой сети ViPNet: установка УКЦ | 2 |
| | **Практическое занятие № 14** Развёртывание защищённой сети ViPNet: установка клиента ViPNet | 2 |
| | **Практическое занятие № 15** Создание структуры защищённой сети ViPNet | 2 |
| | **Практическое занятие № 16** Развёртывание рабочего места помощника главного администратора защищённой сети ViPNet | 2 |
| | **Практическое занятие № 17** Настройка рабочего места помощника главного администратора защищённой сети ViPNet | 2 |
| | **Практическое занятие № 18** Модификация защищённой сети ViPNet | 2 |
| | **Практическое занятие № 19** Компрометация ключей в защищённой сети ViPNet | 2 |
| | **Практическое занятие № 20** Поднятие защищённой сети ViPNet после компрометации | 2 |
| | **Практическое занятие № 21** Настройка политик безопасности в VipNet Policy Manager | 2 |
| | **Практическое занятие № 22** Межсетевое взаимодействие | 2 |
| | **Практическое занятие № 23** Модификация межсетевого взаимодействия в защищённой сети ViPNet | 2 |
| | **Практическое занятие № 24** Составить сравнительную характеристику программно-аппаратных средств для создания защищённой сети | 2 |
| **Тема 3.3 Использование DLP-системы Infowatch для защиты от внутренних утечек информации** | **Содержание учебного материала** | **2** |
| | 3.3.1. Общая характеристика и принципы функционирования dlp-системы Infowatch | 2 |
| | **Практические занятия** | **24** |
| | **Практическое занятие № 25** Установка и настройка Traffic monitor | 2 |
| | **Практическое занятие № 26** Настройка Traffic monitor | 2 |
| | **Практическое занятие № 27** Установка Device monitor | 2 |
| | **Практическое занятие № 28** Настройка Device monitor | 2 |
| | **Практическое занятие № 29** Установка клиента Device monitor. Настройка периметра компании, добавление пользователей и компьютеров в домен | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | **Практическое занятие № 30** Установка и настройка Crawler | 2 |
| | **Практическое занятие № 31** Создание простых правил и проверка их работоспособности в Device monitor | 2 |
| | **Практическое занятие № 32** Создание правил с использованием «белых» и «чёрных» списков в Device monitor | 2 |
| | **Практическое занятие № 33** Добавление ролей, редактирование ролей, удаление ролей в Traffic monitor | 2 |
| | **Практическое занятие № 34** Создание объектов защиты в Traffic monitor | 2 |
| | **Практическое занятие № 35** Изменение объектов защиты в Traffic monitor | 2 |
| | **Практическое занятие № 36** Добавление политик безопасности в Traffic monitor | 2 |
| **Выполнение курсовой работы по теме «Внедрение DLP-системы в организацию» по индивидуальным вариантам** | | **20** |
| **Самостоятельная работа** | | |
| Заполнение рабочей тетради для самостоятельных работ по МДК.03.03 | | 20 |
| **Экзамен** | | **2** |
| **Раздел 4. Основы криптографической защиты данных** | | **72** |
| **Тема 4.1. Основные термины и определения** | **Содержание учебного материала** | **2** |
| | 4.1.1. Основные термины и определения в криптографии. Основные требования, предъявляемые к криптосистемам | 2 |
| **Тема 4.2. Классификация шифров** | **Содержание учебного материала** | **6** |
| | 4.2.1. Шифры замены. Основы шифрования. Шифры однозначной замены. Полиграммные шифры. | 2 |
| | 4.2.2. Шифры перестановки. Шифры гаммирования. Шифры одинарной перестановки. Шифры множественной перестановки. Генерация гаммы. RC4. | 2 |
| | 4.2.3. Шифрование с открытым ключом. Алгоритм RSA. Алгоритм на основе задачи об укладке ранца. Вероятностное шифрование. Алгоритм шифрования Эль-Гамаля. Алгоритм на основе эллиптических кривых. | 2 |
| | **Практические занятия** | **12** |
| | Практическое занятие № 1 Применение шифров перестановки | 2 |
| | Практическое занятие № 2 Алгоритмизация шифра Цезаря | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | Практическое занятие № 3 Декодирование моноалфавитного подстановочного шифра частотным методом | 2 |
| | Практическое занятие № 4 Применение основ модулярной арифметики, проверка простоты и факторизация чисел. | 2 |
| | Практическое занятие № 5 Применение шифров гаммирования | 2 |
| | Практическое занятие № 6 Применение комбинированных шифров | 2 |
| **Тема 4.3. Криптографические протоколы** | **Содержание учебного материала** | **6** |
| | 4.3.1. Протоколы обмена ключами. Алгоритм Диффи-Хеллмана-Меркла. Протоколы аутентификации (идентификации). Хеш-функции. MD5. Применение шифрования для получения хеш-образа. | 2 |
| | 4.3.2. Протоколы электронной цифровой подписи. Протокол на базе алгоритма RSA. Алгоритм цифровой подписи ГОСТ Р 34.10-2001 и ГОСТ Р 34.10-2012. | 2 |
| | 4.3.3. Некоторые сведения из теорий алгоритмов и чисел | 2 |
| | **Практические занятия** | **12** |
| | Практическое занятие № 7 Метод шифрования с открытым ключом RSA | 2 |
| | Практическое занятие № 8 Разработка хэш-функции | 2 |
| | Практическое занятие № 9 Использование шифросистемы Эль-Гамаля | 2 |
| | Практическое занятие № 10 Применение бесключевого протокола Шамира | 2 |
| | Практическое занятие № 11 Применение электронной подписи (ГОСТы 34.10-94 и 34.10-2001) | 2 |
| | Практическое занятие № 12 Настройка ПО для работы с электронной подписью | 2 |
| **Тема 4.4. Основы криптоанализа** | **Содержание учебного материала** | **4** |
| | 4.4.1. Угрозы безопасности при использовании криптографии. Общие сведения о криптоанализе. | 2 |
| | 4.4.2. Методы криптоанализа. Частотный анализ. Метод полного перебора. Методы криптоанализа блочных шифров. Кодирование информации. Общедоступные кодовые системы. Секретные кодовые | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | системы. | |
| | **Практические занятия** | **10** |
| | Практическое занятие № 13 Изучение частотного метода криптоанализа симметричных криптосистем | 2 |
| | Практическое занятие № 14 Изучение методов криптоанализа криптосистем гаммирования с периодической гаммой | 2 |
| | Практическое занятие № 15 Изучение метода линейного криптоанализа блочных симметричных криптосистем | 2 |
| | Практическое занятие № 16 Изучение метода дифференциального (разностного) криптоанализа блочных симметричных криптосистем | 2 |
| | Практическое занятие № 17 Методы оценки качества криптографических генераторов | 2 |
| **Тема 4.5. Стеганография** | **Содержание учебного материала** | **4** |
| | 4.5.1 Классическая стеганография. Компьютерная стеганография | 2 |
| | 4.5.2 Методы сокрытия и обнаружения информации в изображениях, аудиофайлах, видеофайлах | 2 |
| | **Практические занятия** | **16** |
| | Практическое занятие № 18 Применение текстовой криптографии | 2 |
| | Практическое занятие № 19 Исследование методов цифровой стеганографии для защиты информации | 2 |
| | Практическое занятие № 20 Решение ситуационных задач | 2 |
| | Практическое занятие № 21 Применение LSB-стеганографии | 2 |
| | Практическое занятие № 22 Применение метода замены цифровой палитры | 2 |
| | Практическое занятие № 23 Анализ графических изображений на наличие скрытой информации. | 2 |

| Наименование разделов ПМ, МДК и тем | Содержание учебного материала, практические занятия, самостоятельная работа учащихся, производственная практика, курсовое проектирование | Объём часов |
|---|---|---|
| | Практическое занятие № 24 Применение ОС Kali Linux в стеганографии | 2 |
| | Практическое занятие № 25 Решение ситуационных задач | 2 |
| **Самостоятельная работа** | | **4** |
| Заполнение рабочей тетради для самостоятельных работ по МДК.03.04 | | 20 |
| **Дифференцированный зачёт** | | **2** |
| **Учебная практика** | | **72** |
| **Производственная практика** | | **288** |
| **Экзамен по ПМ.04** | | **6** |

## 4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРАКТИКИ

### 4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы профессионального модуля требует наличия лабораторий «Эксплуатации объектов сетевой инфраструктуры»,

Оборудование лаборатории:

- рабочие места по количеству обучающихся;
- рабочее место преподавателя;
- комплект учебно-наглядных пособий, в т.ч. на электронных носителях.

Технические средства обучения:

- компьютеры с лицензионным программным обеспечением на каждом рабочем месте обучающихся и на рабочем месте преподавателя.

### 4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

**Основная литература**


1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. - Москва : КУРС ; ИНФРА-М, 2020. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1071722(дата обращения: 08.04.2021).
2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1189327 (дата обращения: 08.04.2021).
3. Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Электронный ресурс. Режим доступа: сетевой
4. . - URL: https://znanium.com/catalog/product/1189328 (дата обращения: 08.04.2021).
5. Баранова, Е. К. Основы информационной безопасности : учебник/ Е.К. Баранова, А.В. Бабаш. - Москва : РИОР : ИНФРА-М, 2021. — 202 с. — (Среднее профессиональное образование). — DOI: https://doi.org/10.29039/01806-4. - ISBN 978-5-369-01806-4.. - URL: https://znanium.com/catalog/product/1209579 (дата обращения: 08.04.2021).
6. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум / И. Н. Васильева. — Москва : Издательство Юрайт, 2020. — 349 с.— ISBN 978-5-534-02883-6. Электронный ресурс. Режим доступа: сетевой URL: https://urait.ru/bcode/450998 (дата обращения: 08.04.2021).


**Дополнительная литература**


1. Организация сетевого администрирования : учебник / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов, О.А. Ломтева. — Москва : КУРС : ИНФРА-М, 2020. — 384 с. - ISBN 978-5-906818-34-8. - Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1069157 (дата обращения: 08.04.2021).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2020. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Электронный ресурс. Режим доступа: сетевой URL: https://urait.ru/bcode/454453 (дата обращения: 08.04.2021).
3. Богатырев, В. А. Информационные системы и технологии. Теория надежности : учебное пособие для вузов / В. А. Богатырев. — Москва : Издательство Юрайт, 2020. — 318 с. — (Высшее образование). — ISBN 978-5-534-00475-5 Электронный ресурс. Режим доступа: сетевой URL: https://urait.ru/bcode/451108 (дата обращения: 08.04.2021).
4. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2020. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Электронный ресурс. Режим доступа: сетевой — URL: https://urait.ru/bcode/449548 (дата обращения: 08.04.2021).
5. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для СПО / под ред. Т.А. Поляковой, А.А. Стрельцова. - Москва : Издательство Юрайт, 2016. - 325 с. -Серия : Профессиональное образование.
6. Партыка, Т.Л., Попов И.И. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - Москва : ФОРУМ : ИНФРА -М, 2016 - 432 с. : ил. - (Профессиональное образование).
7. Баранова, Е.К., Бабаш А.В. Информационная безопасность и защита информации: Учеб. Пособие. - 3-е изд, перераб. И доп. - Москва : РИОР : ИНФРА-М, 2016. - 322 с. - (Высшее образование).
8. Новиков В.К. Организационно-правовые основы информационной безопасности (защиты информации). Юридическая ответственность за правонарушения в области информационной безопасности (защиты информации). Учебное пособие. - Москва : Горячая линия - Телеком, 2016.- 176 с. : ил.
9. Ищейнов, В.Я., Мецатунян М.В. Основные положения информационной безопасности : учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. -Москва : ФОРУМ : ИНФРА- М, 2017. - 208 с. - (Профессиональное образование).
10. Гришина, Н. В. Основы информационной безопасности предприятия : учеб. пособие / Н.В. Гришина. — Москва : ИНФРА-М, 2019. — 216 с. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/textbook_5cf8ce075a0298.77906820. - ISBN 978-5-16-015105-2. - Электронный ресурс. Режим доступа: сетевой - URL: https://znanium.com/catalog/product/1017663 (дата обращения: 08.04.2021).
11. Конфиденциальное делопроизводство и защищенный электронный документооборот : учебник / Н. Н. Куняев, А. С. Дёмушкин, Т. В. Кондрашова, А. Г. Фабричнов ; под общ. ред. Н. Н. Куняева. - 2-е изд., перераб. и доп. - Москва : Логос, 2020. - 500 с. - (Новая университетская библиотека). - ISBN 978-5-98704-711-8 Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1212394
12. Ищейнов, В. Я. Организационное и техническое обеспечение информационной безопасности. Защита конфиденциальной информации : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - 2-е изд., перераб. и доп. - Москва : ИНФРА-М, 2021. - 256 с. - (Высшее образование: Специалитет). - ISBN 978-5-16-016535-6. - Электронный ресурс.

Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1178151 (дата обращения: 08.04.2021).
13. Минин, И. В. Защита конфиденциальной информации при электронном документообороте/МининИ.В., МининО.В. - Новосибирск : НГТУ, 2011. - 20 с.: ISBN 978-5-7782-1829-1. - Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/546492 (дата обращения: 08.04.2021).
14. Романьков, В. А. Введение в криптографию : курс лекций / В. А. Романьков. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2020. — 240 с. — (Высшее образование: Бакалавриат). - ISBN 978-5-00091-493-9. - Электронный ресурс. Режим доступа: сетевой - URL: https://znanium.com/catalog/product/1046925(дата обращения: 08.04.2021).
15. Информационный мир XXI века. Криптография — основа информационной безопасности : методическое руководство / под ред. Э. А. Болелова ; Московский государственный технический университет гражданской авиации. - 4-е изд. — Москва : Издательско-торговая корпорация «Дашков и К°», 2020. — 126 с. - ISBN 978-5-394-03777-1. Электронный ресурс. Режим доступа: сетевой . - URL: https://znanium.com/catalog/product/1081675(дата обращения: 08.04.2021).

## 5. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)

Формы и методы контроля и оценки результатов обучения должны позволять проверять у учащихся не только получение профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

| **Результаты (освоенные профессиональные компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей. | Корректная настройка, эксплуатация и обслуживание технических и программно-аппаратных средств компьютерных сетей | Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов.<br><br>Экзамен по ПМ. |
| Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях. | Систематический мониторинг работы на объектах сетевой инфраструктуры и рабочих станциях. | Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов.<br><br>Экзамен по ПМ. |
| Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации. | Корректная установка, настройка, эксплуатация и обслуживание сетевых конфигураций | Текущий контроль в форме: устных зачетов по темам; оценки выполнения практических работ; оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов<br>Наблюдения при выполнении практических работ и наблюдение в процессе практики<br><br>Экзамен по ПМ. |

| | | |
|---|---|---|
| Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации. | Разработка схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации | Текущий контроль в форме:<br>устных зачетов по темам;<br>оценки выполнения практических работ;<br>оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов<br>Наблюдения при выполнении практических работ и наблюдение в процессе практики<br><br>Экзамен по ПМ. |
| Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта. | Проведение инвентаризации технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта. | Текущий контроль в форме:<br>устных зачетов по темам;<br>оценки выполнения практических работ;<br>оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов<br><br>Экзамен по ПМ. |
| Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры. | Своевременная замена расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры. | Текущий контроль в форме:<br>устных зачетов по темам;<br>оценки выполнения практических работ;<br>оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов<br><br>Экзамен по ПМ. |
| Применять программно-аппаратные средства защиты информации на защищаемых объектах | Подбор наиболее эффективных программно-аппаратных средств защиты информации на защищаемых объектах | Текущий контроль в форме:<br>устных зачетов по темам;<br>оценки выполнения практических работ;<br>оценки выполнения самостоятельной работы.<br><br>Экспертная оценка разработанных материалов<br><br>Экзамен по ПМ. |
| Участвовать в эксплуатации систем и средств защиты информации защищаемых объектов | Корректная эксплуатация систем и средств защиты информации защищаемых объектов | Текущий контроль в форме: |

| | | |
|---|---|---|
| Применять криптографические аппаратные средства защиты информации на защищаемых объектах | Применение криптографические аппаратные средства защиты информации на защищаемых объектах | устных зачетов по темам; |

| **Результаты (освоенные общие компетенции)** | **Основные показатели оценки результата** | **Формы и методы контроля и оценки** |
|---|---|---|
| ОК 1. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам | Выбор оптимальных способов решения задач профессиональной деятельности, применительно к различным контекстам | Проверка качества выполнения практических работ |
| ОК 2. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности | эффективный поиск необходимой информации; использование различных источников, включая электронные | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие | | |
| ОК 4. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами | взаимодействие с обучающимися, преподавателями в ходе обучения | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста | взаимодействие с обучающимися, преподавателями в ходе обучения | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей. | Корректное взаимодействие с обучающимися, преподавателями в ходе обучения | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК7Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях. | Эффективное использование вычислительных ресурсов | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |

| | | |
|---|---|---|
| ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности. | Использование оптимального соотношения режима труда и отдыха в профессиональной деятельности | Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы |
| ОК 9. Использовать информационно-коммуникационные технологии в профессиональной деятельности | работа с различными прикладными программами | Анализ результатов практических работ |
| ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языках | Работа с профессиональной документацией на государственном и иностранном языках | Проверка качества выполнения практических работ |
| ОК 11Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере | Грамотное использование финансовых ресурсов в профессиональной деятельности | Проверка качества выполнения практических работ |