

**ДЕПАРТАМЕНТ ОБРАЗОВАНИЯ ИВАНОВСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«КИНЕШЕМСКИЙ ТЕХНОЛОГИЧЕСКИЙ КОЛЛЕДЖ»**

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Специальность

09.02.06 Сетевое и системное администрирование

Уровень подготовки – базовый

Квалификация - специалист по администрированию сети

2022г.

Рабочая программа профессионального модуля разработана на основе Федерального государственного образовательного стандарта (далее – ФГОС) среднего профессионального образования (далее – СПО) по специальности **09.02.06 Сетевое и системное администрирование.**

Составитель:

Ветюгов Александр Викторович, преподаватель
фамилия, инициалы, должность

Рассмотрена на заседании учебно-методического объединения по укрупненным группам специальностей 09.00.00 Информатика и вычислительная техника, 13.00.00 Электро- и теплоэнергетика, 15.00.00 Машиностроение, 18.00.00 Химические технологии

Протокол № 1 от «31» августа 2022 г.

Рекомендована Методическим советом

Протокол № 1 от «31» августа 2022 г.

СОДЕРЖАНИЕ

	стр.
1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	3
2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	5
3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ	11
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)	13

**1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ
ПМ.03 ЭКСПЛУАТАЦИЯ ОБЪЕКТОВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ**

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля студент должен освоить основной вид деятельности выполнение работ по проектированию сетевой инфраструктуры и соответствующие ему общие компетенции, профессиональные компетенции:

1.1.1. Перечень общих компетенций

Код	Наименование общих компетенций
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 общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
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 поддержания необходимого уровня физической подготовленности.
ОК 9.	Использовать информационные технологии в профессиональной деятельности
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языках.
ОК 11.	Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.

1.1.2. Перечень профессиональных компетенций

Код	Наименование видов деятельности и профессиональных компетенций
ВД 3.	<i>Эксплуатация объектов сетевой инфраструктуры</i>
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.
---------	---

1.1.3. В результате освоения профессионального модуля студент 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
знать	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных сетей; методы устранения неисправностей в технических средствах

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов 758

Из них на освоение МДК. 03.01 276

на освоение МДК. 03.02 230

на практики, в том числе учебную 72 и производственную 180

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.					Промежуточная аттестация	Самостоятельная работа
			Обучение по МДК			Практики			
			Всего	Лабораторных и практических занятий	Курсовых проектов	Учебная	Производственная		
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>	<i>8</i>	<i>9</i>	<i>10</i>
ОК 01-11 ПК 3.1-3.6	Раздел 1. Эксплуатация объектов сетевой инфраструктуры	276	276	76	30	-	-	-	-
ОК 01-11 ПК 3.1-3.6	Раздел 2. Безопасность компьютерных сетей	230	230	60	-	-	-	-	-
ОК 01-11 ПК 3.1-3.6	Учебная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	72				72	-	-	-
ОК 01-11 ПК 3.1-3.6	Производственная практика (по профилю специальности), часов (если предусмотрена итоговая (концентрированная) практика)	180				180	-	-	-
	Всего:	758	506	136	30	72	180	-	-

2.2. Тематический план и содержание профессионального модуля (ПМ.03)

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) (если предусмотрены)	Объём в часах
1	2	3
Раздел 1. Эксплуатация объектов сетевой инфраструктуры		
МДК. 03.01. Эксплуатация объектов сетевой инфраструктуры		276
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры	<p><i>Содержание</i></p> <ol style="list-style-type: none"> 1. Физические аспекты эксплуатации. Физическое вмешательство в инфраструктуру сети. 2. Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки. 3. Полоса пропускания, паразитная нагрузка. 4. Расширяемость сети. Масштабируемость сети. 5. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб). 6. Нарастивание длины сегментов сети; замена существующей аппаратуры. 7. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети. 8. Техническая и проектная документация. Паспорт технических устройств. 9. Физическая карта всей сети; логическая топология компьютерной сети. 10. Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры. 11. Проверка объектов сетевой инфраструктуры и профилактические работы. 12. Проведение регулярного резервирования. 13. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках. 14. Программное обеспечение мониторинга компьютерных сетей и сетевых устройств. 15. Протокол SNMP, его характеристики, формат сообщений, набор услуг. 16. Задачи управления: анализ производительности и надежности сети. 17. Задачи управления: анализ производительности и надежности сети. 18. Задачи управления: анализ производительности и надежности сети. 	142

19. Задачи управления: анализ производительности и надежности сети.	
20. Оборудование для диагностики и сертификации кабельных систем.	
21. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	
22. Сетевые протоколы уровня приложений (DNS, FTP, HTTP, SNMP).	
23. Основы работы системы доменных имен (DNS).	
24. Принципы работы NAT и PAT.	
25. Методы обеспечения отказоустойчивости оборудования.	
26. Мониторинг состояния оборудования.	
27. Основные причины отказов сетевого оборудования.	
28. Подходы к диагностике и устранению неисправностей.	
29. Программное обеспечение для управления сетевой инфраструктурой.	
30. Средства резервного копирования сетевых конфигураций.	
31. Основы управления конфигурациями сетевых устройств.	
32. Программное обеспечение для анализа трафика (Wireshark, NetFlow).	
33. Принципы построения беспроводных сетей.	
34. Основные стандарты Wi-Fi и их особенности.	
35. Точки доступа: функции и настройка.	
36. Методы повышения безопасности беспроводных сетей.	
37. Организация сегментирования сети.	
38. Политики управления доступом (ACL).	
39. Межсетевые экраны: функции и назначение.	
40. Методы шифрования данных в сетевой инфраструктуре.	
41. VPN: назначение, виды и принципы работы.	
42. Средства предотвращения и устранения сетевых атак.	
43. Основы построения отказоустойчивых сетей.	
44. Применение технологий резервирования (HSRP, VRRP).	
45. Организация систем охлаждения и энергоснабжения оборудования.	
46. Подходы к модернизации сетевого оборудования.	
47. Аудит сетевой инфраструктуры: основные этапы.	
48. Документирование сетевых решений и конфигураций.	
49. Перспективы развития сетевых технологий.	
50. Рекомендации по обновлению и оптимизации инфраструктуры.	
В том числе практических занятий	42
Практическое занятие 1. Оконцовка кабеля витая пара.	
Практическое занятие 2. Заделка кабеля витая пара в розетку.	

	Практическое занятие 3 . Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену.	
	Практическое занятие 4. Тестирование кабеля.	
	Практическое занятие 5. Поддержка пользователей сети.	
	Практическое занятие 6. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы).	
	Практическое занятие 7. Выполнение действий по устранению неисправностей.	
	Практическое занятие 8. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	
	Практическое занятие 9. Оформление технической документации, правила оформления документов.	
	Практическое занятие 10. Протокол управления SNMP.	
	Практическое занятие 11. Основные характеристики протокола SNMP.	
	Практическое занятие 12. Набор услуг (PDU) протокола SNMP.	
	Практическое занятие 13 . Формат сообщений SNMP.	
	Практическое занятие 14. Задачи управления: анализ производительности сети.	
	Практическое занятие 15. Задачи управления: анализ надежности сети.	
	Практическое занятие 16. Управление безопасностью в сети.	
	Практическое занятие 17. Учет трафика в сети.	
	Практическое занятие 18. Средства мониторинга компьютерных сетей.	
	Практическое занятие 19. Средства анализа сети с помощью команд сетевой операционной системы Windows.	
	Практическое занятие 20. Средства анализа сети с помощью команд сетевой операционной системы Linux.	
	Практическое занятие 21.Финальная комплексная практическая работа по эксплуатации объектов сетевой инфраструктуры.	
Тема 1.2. Эксплуатация систем IP-телефонии	Содержание	104
	1. Настройка H.323. Описание H.323 и общие рекомендации.	
	2. Функциональные компоненты H.323.Установка и поддержка соединения H.323.	
	3. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper.	
	4. Многопользовательские конференции. Обеспечение отказоустойчивости.	
	5. Настройка SIP. Описание и общие рекомендации.	
	6. Технология SIP и связанные с ней стандарты.	
	7. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP.	
	8. Модель установления соединения. Планирование отказоустойчивости.	
	9. Установка и инсталляция программного коммутатора.	
	10. Монтажные процедуры. Процедуры инсталляции.	
	11. Управление аппаратными средствами и портами.	
	12. Протоколы управления MGCP, H.248. Создание аналоговых абонентов.	

13. Внутростанционная маршрутизация.	
14. Управление программным коммутатором.	
15. Маршрутизация. Группы соединительных линий.	
16. Подключение станций с TDM (абонентский доступ TDM).	
17. Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP - абоненты.	
18. Группы абонентов. Дополнительные абонентские услуги.	
19. Организация эксплуатации систем IP-телефонии.	
20. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	
21. Восстановление работы сети после аварии.	
22. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных.	
23. Развертывание сети с использованием VLAN для IP-телефонии.	
24. Настройка шлюза.	
25. Установка, подключение и первоначальные настройки голосового маршрутизатора.	
26. Настройка таблицы пользователей в голосовом маршрутизаторе.	
27. Настройка групп в голосовом маршрутизаторе.	
28. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе.	
29. Настройка голосовых сообщений в маршрутизаторе.	
30. Настройка программно-аппаратной IP-АТС.	
31. Установка и настройка программной IP-АТС (например, Asterisk).	
32. Тестирование кодеков. Исследование параметров качества обслуживания.	
33. Мониторинг и анализ соединений по различным протоколам.	
34. Мониторинг вызовов в программном коммутаторе.	
35. Создание резервных копий баз данных.	
В том числе практических занятий	22
Практическое занятие 1. Настройка аппаратных IP-телефонов.	
Практическое занятие 2. Настройка программных IP-телефонов, факсов.	
Практическое занятие 3. Развертывание сети с использованием VLAN для IP-телефонии.	
Практическое занятие 4. Установка, подключение и первоначальные настройки голосового маршрутизатора.	
Практическое занятие 5. Настройка таблицы пользователей в голосовом маршрутизаторе.	
Практическое занятие 6. Настройка групп в голосовом маршрутизаторе.	
Практическое занятие 7. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе.	
Практическое занятие 8. Настройка голосовых сообщений в маршрутизаторе.	
Практическое занятие 9. Установка и настройка программной IP-АТС (например, Asterisk).	
Практическое занятие 10. Диагностика и устранение неисправностей в системах IP-телефонии.	

Тема 2.3. Курсовой проект (обязательные учебные занятия)	Практическое занятие 11. Финальная комплексная практическая работа по эксплуатации систем IP-телефонии.	30
	Содержание	
	<i>1. Выбор типа и топологии сети. (К/н)</i>	
	<i>2. Выбор оборудования и типа кабеля. (К/н)</i>	
	<i>3. Выбор программного обеспечения. (К/н)</i>	
	<i>4. Разработка плана расположения оборудования и прокладки кабеля. (К/н)</i>	
	<i>5. Описание логической топологии сети. (К/н)</i>	
	<i>6. Описание взаимодействия серверов компьютерной сети и рабочих станций. (К/н)</i>	
	<i>7. Описание строится на основе графического изображения логической топологии. Пример описания: Сервера должны быть разделены: каждый сервер – отдельный сегмент сети. Между серверами должно быть соединение. Пользователи из различных подсетей не должны/должны иметь доступ друг к другу (пример: сегмент бухгалтерии, сегмент кассиров/операторов, сегмент склада и т.д.). (К/н)</i>	
	<i>8. Расчет необходимого количества оборудования. (К/н)</i>	
	<i>9. Мероприятия по эксплуатации сетевой инфраструктуры. В разделе приводятся стандарты по эксплуатации сетевого оборудования. (К/н)</i>	
	<i>10. Мониторинг и диагностика сети. Установка и настройка систем мониторинга (Zabbix, PRTG, Nagios). Методы диагностики сетевых проблем. (К/н)</i>	
	<i>11. Организация резервного копирования. Планирование резервирования данных. Выбор и настройка решений для бэкапа. (К/н)</i>	
	<i>12. Разработка плана обслуживания сети. Регламент технического обслуживания. График профилактических работ. (К/н)</i>	
<i>13. Тестирование и проверка работоспособности. Сценарии тестирования сети. Анализ полученных результатов. (К/н)</i>		
<i>14. Экономическая оценка проекта. Расчет затрат на оборудование, ПО и обслуживание. Оценка окупаемости проекта. (К/н)</i>		

	<i>15.Графическая часть проекта. Разработка схемы топологии сети (Логическая структура (уровни сети, основные узлы, соединения). Физическая структура (размещение оборудования, точки подключения). Подготовка таблиц и диаграмм (Таблицы IP-адресов и настроек VLAN). Диаграммы маршрутизации и потоков данных. Создание схем организации резервного копирования. Иллюстрация процесса мониторинга сети (Снимки интерфейсов систем мониторинга). Примеры отчетов и графиков. Оформление графических элементов в соответствии с требованиями ГОСТ. (К/п)</i>	
МДК.03.02. Безопасность компьютерных сетей		230
Тема 2.1 Безопасность компьютерных сетей	Содержание	230
	1.Фундаментальные принципы безопасной сети.	
	2. Современные угрозы сетевой безопасности.	
	3. Вирусы, черви и троянские кони.	
	4. Методы атак.	
	5. Обеспечение безопасности в сети.	
	6. Нейтрализация угроз.	
	7. Безопасность Сетевых устройств OSI.	
	8. Безопасный доступ к устройствам.	
	9. Защита доступа к устройствам.	
	10. Назначение административных ролей.	
	11. Мониторинг и управление устройствами.	
	12. Использование функция автоматизированной настройки безопасности.	
	13.Использование автоматических функций обеспечения безопасности.	
	14. Защита плоскости управления.	
	15. Авторизация, аутентификация и учет доступа (AAA).	
	16. Свойства AAA.	
	17. Локальная AAA аутентификация.	
	18. Server-based AAA.	
	19. Локальная аутентификация AAA.	
	20. Серверное решение AAA.	
	21. Серверная аутентификация AAA.	
	22. Серверная авторизация и учет AAA.	
	23. Исследование методов шифрования.	
	24. Реализация технологий брандмауэра.	
	25. ACL. Технология брандмауэра.	

26. Контекстный контроль доступа (СВАС).
27. Политики брандмауэра, основанные на зонах.
28. Реализация технологий предотвращения вторжения.
29. IPS технологии.
30. IPS сигнатуры.
31. Реализация IPS.
32. Проверка и мониторинг IPS.
33. Безопасность локальной сети.
34. Обеспечение безопасности пользовательских компьютеров.
35. Соображения по безопасности второго уровня (Layer-2).
36. Конфигурация безопасности второго уровня.
37. Безопасность беспроводных сетей, VoIP и SAN.
38. Факторы, которые необходимо учитывать при обеспечении безопасности на втором уровне.
39. Криптографические системы.
40. Криптографические сервисы.
41. Базовая целостность и аутентичность.
42. Конфиденциальность.
43. Криптография открытых ключей.
44. Определение VPN. Разновидности VPN-технологий.
45. Реализации VPN-технологий. Схемы использования VPN - технологий.
46. Топологии VPN.
47. Краткие сведения об IPsec.
48. Протокол L2TP. Протокол PPTP.
49. Сертифицированные решения для построения VPN.
50. Внедрение виртуальных частных сетей (VPN).
51. Реализация технологий VPN.
52. VPN.
53. GRE VPN.
54. Компоненты и функционирование IPSec VPN.
55. Реализация Site-to-site IPSec VPN с использованием CLI.
56. Реализация Site-to-site IPSec VPN с использованием CCP.
57. Реализация Remote-access VPN.
58. Управление безопасной сетью.
59. Принципы безопасности сетевого дизайна.
60. Безопасная архитектура.

61. Управление процессами и безопасность.	
62. Тестирование сети на уязвимости.	
63. Непрерывность бизнеса, планирование восстановления аварийных ситуаций.	
64. Жизненный цикл сети и планирование.	
65. Разработка регламентов компании и политик безопасности.	
66. Cisco ASA.	
67. Введение в адаптивное устройство безопасности ASA.	
68. Конфигурация фаервола на базе ASA с использованием графического интерфейса ASDM.	
69. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.	
70. Обнаружение сетевых атак. Архитектура систем обнаружения атак.	
71. Классификация систем обнаружения атак.	
72. Анализ сигнатур. Виды сигнатур.	
73. Примеры систем обнаружения атак. Система обнаружения атак Snort.	
74. Общие меры безопасности применяемые для защиты от атаки на сервера в сети.	
75. Общие проблемы безопасности служб прикладного уровня.	
76. Уязвимости протокола DHCP. Обнаружение ложного DHCP-сервера.	
77. Изучение механизма DNS Spoofing.	
78. Honeynet или сеть-приманка для изучения поведения нарушителей.	
79. Классификация сетей-приманок, практические реализации. Принципы организации Honeynet.	
80. Утилита honeypd, проект HoneyNet. Сценарии использования сетей-приманок (обнаружение сетевых червей, контроль распространении спама и т. д.).	
81. Финальная комплексная лабораторная работа по безопасности.	
В том числе практических занятий	60
Практическая работа 1. Социальная инженерия.	
Практическая работа 2. Исследование сетевых атак и инструментов проверки защиты сети.	
Практическая работа 3. Изучение сетевых атак и инструментов аудита безопасности.	
Практическая работа 4. Защита маршрутизатора для административного доступа.	
Практическая работа 5. Packet Trace. Конфигурирование маршрутизатора Cisco для использования Syslog, NTP и SSH.	
Практическая работа 6. Packet Trace. Настройка расширенных ACL – списков по сценарию 1.	
Практическая работа 7. Packet Trace. Настройка расширенных ACL – списков по сценарию 2.	
Практическая работа 9. Настройка безопасного доступа к маршрутизатору.	
Практическая работа 10. Обеспечение административного доступа AAA и сервера Radius.	
Практическая работа 11. Защита административного доступа с помощью AAA и RADIUS.	
Практическая работа 12. Packet Tracer. Настройка аутентификации AAA на маршрутизаторах Cisco.	

Практическая работа 13. Настройка политики безопасности брандмауэров.
Практическая работа 14. Настройка Site-to-SiteVPN используя интерфейс командной строки.
Практическая работа 15. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки.
Практическая работа 16. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM.
Практическая работа 17. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM.
Практическая работа 18. Настройка Clientless Remote Access SSL VPNs используя ASDM.
Практическая работа 19. Настройка AnyConnect Remote Access SSL VPN используя ASDM.
Практическая работа 20. Настройка системы предотвращения вторжений (IPS).
Практическая работа 21. <i>Конфигурирование IOS IPS с использованием интерфейса командной строки.</i>
Практическая работа 22. Настройка безопасности на втором уровне на коммутаторах.
Практическая работа 23. <i>Защита коммутаторов второго уровня.</i>
Практическая работа 24. <i>Packet Tracer. Обеспечение безопасности на 2-м уровне. Packet Tracer. Безопасность VLAN на 2-м уровне.</i>
Практическая работа 25. <i>Изучение методов шифрования.</i>
Практическая работа 26. Настройка Site-to-SiteVPN используя интерфейс командной строки.
Практическая работа 27. <i>Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI) 1.</i>
Практическая работа 28. <i>Конфигурирование базовых настроек ASA и межсетевого экрана с использованием интерфейса командной строки (CLI) 2.</i>
Практическая работа 29. <i>Конфигурирование базовых настроек ASA и межсетевого экрана с использованием ASDM 1.</i>
Практическая работа 30. <i>Конфигурирование базовых настроек ASA и межсетевого экрана с использованием ASDM. 2.</i>

	<p>Учебная практика Виды работ</p> <ol style="list-style-type: none"> 1. Настройка прав доступа. 2. Оформление технической документации, правила оформления документов. 3. Настройка аппаратного и программного обеспечения сети. 4. Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain. 5. Программная диагностика неисправностей. 6. Аппаратная диагностика неисправностей. 7. Поиск неисправностей технических средств. 8. Выполнение действий по устранению неисправностей. 9. Использование активного, пассивного оборудования сети. 10. Устранение паразитирующей нагрузки в сети. 11. Построение физической карты локальной сети. 12. Дифференцированный зачет. Оформление отчета. 	72
--	---	----

<p>Производственная практика раздела Примерный перечень работ:</p> <ol style="list-style-type: none"> 1. Введение в производственную практику. Ознакомление с целью и задачами практики. Знакомство с организацией и ее сетевой инфраструктурой. Изучение техники безопасности при работе с сетевым оборудованием. 2. Изучение нормативной документации. Ознакомление с локальными нормативными актами и регламентами. Анализ документации на сетевую инфраструктуру (топологии, спецификации оборудования). 3. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение. 4. Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях. 5. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций. 6. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли. 7. Установка прав доступа и контроль использования сетевых ресурсов. 8. Обеспечение своевременного копирования, архивирования и резервирования данных. 9. Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. 10. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению. 11. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети. 12. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия. 13. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций. 14. Документирование всех произведенных действий. 15. Работа с коммутаторами и маршрутизаторами. Настройка VLAN и маршрутизации. Проверка таблиц маршрутов. 16. Мониторинг сетевой инфраструктуры. Использование инструментов мониторинга (Zabbix, PRTG). Анализ сетевых метрик и логов. 17. Резервное копирование и восстановление конфигураций. Проверка системы резервного копирования. Проведение тестов восстановления данных. 18. Работа с беспроводными сетями. Настройка точек доступа и проверка их работоспособности Диагностика беспроводных подключений. 19. Управление доступом. Настройка списков управления доступом (ACL). Анализ текущих правил фильтрации. 20. Обновление сетевого оборудования и программного обеспечения. Изучение процесса обновления прошивок и ПО. Выполнение обновлений. 21. Анализ сетевых атак и их предотвращение. Изучение журналов безопасности. Реализация мер защиты от атак. 22. Техническое обслуживание оборудования. Очистка от пыли, проверка состояния кабелей. Замена поврежденных компонентов. 23. Документирование сети. Создание и обновление схем топологии сети. Ведение журналов изменений конфигураций. 24. Обеспечение отказоустойчивости сети. Настройка резервирования (HSRP, VRRP). Тестирование работы в случае отказа оборудования. 25. Интеграция новых устройств в сеть. Подключение нового оборудования. Настройка и тестирование взаимодействия. 26. Проверка безопасности межсетевого взаимодействия. Настройка межсетевых экранов. Тестирование доступа между сегментами. 27. Организация кабельной инфраструктуры. Проверка кабелей и разъемов. Участие в монтажных работах. 28. Проведение тестирования сети. Анализ пропускной способности. Определение узких мест. 29. Участие в проектировании сети. Разработка схем для расширения или улучшения сети. Подготовка предложений по модернизации. 30. Подведение итогов производственной практики. Подготовка отчетности. Дифференцированный зачет. 	<p>180</p>
<p>Всего</p>	<p>758</p>

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля предусмотрено следующее специальное помещение:

Лаборатория организация и принципы построения компьютерных систем, оснащенная:

- 12-15 компьютеров обучающихся и 1 компьютер преподавателя (аппаратное обеспечение: не менее 2 сетевых плат, процессор не ниже Core i3, оперативная память объемом не менее 8 Гб; HD 500 Gb или больше программное обеспечение: операционные системы Windows, UNIX, пакет офисных программ, пакет САПР);

Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа, обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-ножи, кросс-панели;

- Пример проектной документации;
- Необходимое лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности;

- Сервер в лаборатории (аппаратное обеспечение: не менее 2 сетевых плат, 8-х ядерный процессор с частотой не менее 3 ГГц, оперативная память объемом не менее 16 Гб, жесткие диски общим объемом не менее 2 Тб, программное обеспечение: Windows Server 2012 или более новая версия, лицензионные антивирусные программы, лицензионные программы восстановления данных, лицензионные программы по виртуализации.)

- Технические средства обучения:
- Компьютеры с лицензионным программным обеспечением
- Интерактивная доска
- 6 маршрутизаторов, обладающих следующими характеристиками:

ОЗУ не менее 256 Мб с возможностью расширения

ПЗУ не менее 128 Мб с возможностью расширения

USB порт: не менее одного стандарта USB 1.1

Встроенные сетевые порты: не менее 2-х Ethernet скоростью не менее 100Мб/с.

Внутренние разъёмы для установки дополнительных модулей расширения: не менее двух для модулей AIM.

Консольный порт для управления маршрутизатором через порт стандарта RS232.

Встроенное программное обеспечение должно поддерживать статическую и динамическую маршрутизацию.

Маршрутизатор должен поддерживать управление через локальный последовательный порт и удалённо по протоколу telnet.

Иметь сертификаты безопасности и электромагнитной совместимости:

UL 60950, CAN/CSA C22.2 No. 60950, IEC 60950, EN 60950-1, AS/NZS 60950, EN300386, EN55024/CISPR24, EN50082-1, EN61000-6-2, FCC Part 15, ICES-003 Class A, EN55022 Class A, CISPR22 Class A, AS/NZS 3548 Class A, VCCI Class A, EN 300386, EN61000-3-3, EN61000-3-2, FIPS 140-2 Certification

6 коммутаторов, обладающих следующими характеристиками:

Коммутатор с 24 портами Ethernet со скоростью не менее 100 Мб/с и 2 портами Ethernet со скоростью не менее 1000Мб/с

В коммутаторе должен присутствовать разъём для связи с ПК по интерфейсу RS-232. При использовании нестандартного разъёма в комплекте должен быть соответствующий кабель или переходник для COM разъёма.

Скорость коммутации не менее 16Gbps

ПЗУ не менее 32 Мб

ОЗУ не менее 64Мб

Максимальное количество VLAN 255

Доступные номера VLAN 4000

Поддержка протоколов для совместного использования единого набора VLAN на группе коммутаторов.

Размер MTU 9000б

Скорость коммутации для 64 байтных пакетов 6.5*10⁶ пакетов/с

Размер таблицы MAC-адресов: не менее 8000 записей

Количество групп для IGMP трафика для протокола IPv4 255

Количество MAC-адресов в записях для службы QoS: 128 в обычном режиме и 384 в режиме QoS.

Количество MAC-адресов в записях контроля доступа: 384 в обычном режиме и 128 в режиме QoS.

Коммутатор должен поддерживать управление через локальный последовательный порт, удалённое управление по протоколу Telnet, Ssh.

В области взаимодействия с другими сетевыми устройствами, диагностики и удалённого управления

RFC 768 — UDP, RFC 783 — TFTP, RFC 791 — IP, RFC 792 — ICMP, RFC 793 — TCP, RFC 826 — ARP, RFC 854 — Telnet, RFC 951 - Bootstrap Protocol (BOOTP), RFC 959 — FTP, RFC 1112 - IP Multicast and IGMP, RFC 1157 - SNMP v1, RFC 1166 - IP Addresses, RFC 1256 - Internet Control Message Protocol (ICMP) Router Discovery, RFC 1305 — NTP, RFC 1493 - Bridge MIB, RFC 1542 - BOOTP extensions, RFC 1643 - Ethernet Interface MIB, RFC 1757 — RMON, RFC 1901 - SNMP v2C, RFC 1902-1907 - SNMP v2, RFC 1981 - Maximum Transmission Unit (MTU) Path Discovery IPv6, RFC 2068 — HTTP, RFC 2131 — DHCP, RFC 2138 — RADIUS, RFC 2233 - IF MIB v3, RFC 2373 - IPv6 Aggregatable Addrs, RFC 2460 — IPv6, RFC 2461 - IPv6 Neighbor Discovery, RFC 2462 - IPv6 Autoconfiguration, RFC 2463 - ICMP IPv6, RFC 2474 - Differentiated Services (DiffServ) Precedence, RFC 2597 - Assured Forwarding, RFC 2598 - Expedited Forwarding, RFC 2571 - SNMP Management, RFC 3046 - DHCP Relay Agent Information Option

RFC 3376 - IGMP v3, RFC 3580 - 802.1X RADIUS.

Иметь сертификаты безопасности и электромагнитной совместимости:

UL 60950-1, Second Edition, CAN/CSA 22.2 No. 60950-1, Second Edition, TUV/GS to EN 60950-1, Second Edition, CB to IEC 60950-1 Second Edition with all country deviations, CE Marking, NOM (through partners and distributors), FCC Part 15 Class A, EN 55022 Class A (CISPR22), EN 55024 (CISPR24), AS/NZS CISPR22 Class A, CE, CNS13438 Class A, MIC, GOST, China EMC Certifications.

- телекоммуникационная стойка (шасси, сетевой фильтр, источники бесперебойного питания);
- 2 беспроводных маршрутизатора Linksys (предпочтительно серии EA 2700, 3500, 4500) или аналогичные устройства SOHO
- IP телефоны от 3 шт.
- Программно-аппаратные шлюзы безопасности от 2 шт.
- 1 компьютер для лабораторных занятий с ОС Microsoft Windows Server, Linux и системами виртуализации

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы, рекомендуемые для использования в образовательном процессе.

3.2.1. Печатные издания

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. - Москва : КУРС ; ИНФРА-М, 2020. — 360 с.

3.2.2. Электронные издания (электронные ресурсы)

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгальчев, В.П. Мельников. - Москва : КУРС ; ИНФРА-М, 2020. — 360 с. — (Среднее профессиональное образование). - ISBN 978-5-906923-06-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1071722> (дата обращения: 26.07.2021). – Режим доступа: по подписке.

3.3. Кадровое обеспечение образовательного процесса

Требования к квалификации педагогических кадров, обеспечивающих обучение по профессиональному модулю: реализация профессионального модуля обеспечивается педагогическими кадрами, имеющими высшее образование, соответствующее профилю профессионального модуля.

Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным для преподавателей, отвечающих за освоение обучающимися профессионального модуля, эти преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ (ВИДА ДЕЯТЕЛЬНОСТИ)

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
<p><i>ПК 3.1.</i> Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.</p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>
<p><i>ПК 3.2.</i> Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.</p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>

	заданию.	
<p><i>ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации</i></p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>

<p><i>ПК 3.4.</i> Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.</p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>
<p><i>ПК 3.5.</i> Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.</p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>

<p><i>ПК 3.6.</i> Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.</p>	<p>Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры.</p> <p>Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры.</p> <p>Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.</p>	<p>Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием</p> <p>Защита отчетов по практическим и лабораторным работам</p>
---	---	---

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	<ul style="list-style-type: none"> – обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач 	<p>Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы</p> <p>Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен квалификационный</p>
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - 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.	<ul style="list-style-type: none"> - грамотность устной и письменной речи, - ясность формулирования и изложения мыслей 	
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	<ul style="list-style-type: none"> - соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик, - соблюдение стандартов антикоррупционного поведения 	
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	<ul style="list-style-type: none"> - 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 поддержания необходимого уровня физической подготовленности.;	<ul style="list-style-type: none"> - эффективно использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.; 	

ние необходимого уровня физической подготовленности.		
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.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	
ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.	-эффективно использовать знания по финансовой грамотности, - эффективно планировать предпринимательскую деятельность в профессиональной сфере при проведении работ по конструированию сетевой инфраструктуры	

Преподаватель _____ А.В. Ветюгов

(занимаемая должность)

(подпись)

(инициалы, фамилия)

