Приложение 1

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 01. Выполнение работ по проектированию сетевой инфраструктуры

Специальность: 09.02.06 Сетевое и системное администрирование

2020г.

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 01. Выполнение работ по проектированию сетевой инфраструктуры

1.1. Область применения программы профессионального модуля

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности: 09.02.06 Сетевое и системное администрирование.

1.2. Цели и задачи профессионального модуля – требования к результатам 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**:

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.

ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. 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.

Выпускник, освоивший программу СПО по специальности 09.02.06 Сетевое и системное администрирование, должен обладать **профессиональными компетенциями:**

ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети.

ПК 1.2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.

ПК 1.3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.

ПК 1.4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.

ПК 1.5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.

В результате освоения профессионального модуля студент должен:

иметь практический опыт:

– проектировании архитектуры локальной сети в соответствии с поставленной задачей;

– установке и настройке сетевых протоколов и сетевого оборудования в соответствии с конкретной задачей;

– выборе технологии, инструментальных средств при организации процесса исследования объектов сетевой инфраструктуры;

– обеспечении безопасного хранения и передачи информации в локальной сети;

– использовании специального программного обеспечения для моделирования, проектирования и тестирования компьютерных сетей.

уметь:

– проектировать локальную сеть, выбирать сетевые топологии;

– использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети.

знать:

– общие принципы построения сетей, сетевых топологий, многослойной модели OSI, требований к компьютерным сетям;

– архитектуру протоколов, стандартизации сетей, этапов проектирования сетевой инфраструктуры;

– базовые протоколы и технологии локальных сетей;

– принципы построения высокоскоростных локальных сетей;

– стандарты кабелей, основные виды коммуникационных устройств, терминов, понятий, стандартов и типовых элементов структурированной кабельной системы.

1.3. Рекомендуемое количество часов на освоение программы профессионального модуля:

Общая нагрузка – **801 ч**., в том числе:
самостоятельная работа – **23 ч.**;
теоретические занятия– **90 ч.**;
практические занятия – **174 ч.**;
консультации – **10 ч.**;
учебная практика – **216 ч.;**
производственная практика – **216 ч;**
Курсовая работа – **30 ч.**
Квалификационный экзамен **– 18 ч.**

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Общая	Учебная нагрузка							Практики	
			Самостоятельная работа	во взаимодействии с преподавателями						Учебная	Производственная
				Всего по МДК	в том числе						
					Теоретическое обучение	Лаб. Практ.	Курсов. работа	Консультации	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11	12
ПК 1.1-ПК 1.5 ОК 01-ОК 11	**Раздел1.** Компьютерные сети	*176*	*8*	*168*	*68*	*84*		*4*	*12*		
ПК 1.1-ПК 1.5 ОК 01-ОК 11	**Раздел2.** Организация, принципы построения и функционирования компьютерных сетей	*175*	*15*	*160*	*22*	*90*	*30*	*6*	*12*		
ПК 1.1-ПК 1.5 ОК 01-ОК 11	Учебная практика	*216*								*216*	
ПК 1.1-ПК 1.5 ОК 01-ОК 11	Производственная практика	*216*									*216*
	Квалификационный экзамен	*18*		*18*					*18*		
	Всего	*801*	*23*		*90*	*174*	*30*	*10*	*42*	*216*	*216*

2.2. Тематический план и содержание профессионального модуля ПМ 01. Выполнение работ по проектированию сетевой инфраструктуры

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа	Объем часов	Коды компетенций
1		**2**	**3**	**4**
Раздел 1. МДК 01.01. Компьютерные сети			***168/84(8)***	
5 семестр			***128/58(8)***	
Тема 1.	**Введение в сетевые технологии**		***90/48(8)***	
Тема 1.1. Компьютерные сети		**Содержание учебного материала**		
	1	Компьютерные сети. Совместная работа, Интернет и современные сетевые технологии – область применения и назначение. Тенденции развития сетей. Виды компьютерных сетей. Глобальные и локальные сети. Одноранговые и клиент-серверные архитектуры. Основные компоненты сетей, сетевая среда и сетевые устройства.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.2. Технологии подключения к Интернет. Качество и надежность сетей.		**Содержание учебного материала**		
	2	Технологии подключения к Интернет. Конвергентные сети. Качество и надежность сетей. Основные понятия сетевой безопасности. Кодирование и параметры сообщения. Консольный доступ, удаленный доступ с помощью Telnet и SSH, использование порта AUX. Организации по стандартизации: ISOC, IAB, IETF, IEEE, ISO.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.3. Многоуровневые модели OSI и TCP/IP		**Содержание учебного материала**		
	3	Многоуровневые модели OSI и TCP/IP. Инкапсуляция данных. Протокольные блоки данных (PDU). Доступ к локальным ресурсам. MAC- и IP- адреса. Доступ к удалённым ресурсам. Шлюз по умолчанию.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.4. Протоколы и стандарты физического уровня		**Содержание учебного материала**		
	4	Протоколы и стандарты физического уровня. Способы подключения к сети. Сетевые интерфейсные платы (NIC). Среды передачи данных и их характеристики: пропускная способность, производительность.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.5. Разновидности, особенности		**Содержание учебного материала**		
	5	Виды медных сетевых кабелей: UTP, STP, коаксиальный. Разновидности,	*2*	*ОК 01 –*

прокладки и тестирования кабелей		особенности прокладки и тестирования кабелей. Структура и особенности прокладки оптоволоконных кабелей. Беспроводные средства передачи данных. Стандарт Wi-Fi IEEE 802.11.		*ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.6. Канальный уровень и его подуровни		**Содержание учебного материала**		
	6	Канальный уровень и его подуровни: Управление логическим каналом (LLC) и Управление доступом к среде передачи данных MAC. Структура кадра канального уровня и принципы его формирования. Стандарты канального уровня.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.7. Физическая и логическая топология сети		**Содержание учебного материала**		
	7	Физическая и логическая топология сети. Топологии «точка-точка», «звезда», «полносвязанная», «кольцевая». Полудуплексная и полнодуплексная передача данных. Особенности кадров LAN, WAN, Ethernet, PPP, 802.11.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.8. Семейство сетевых технологий Ethernet.		**Содержание учебного материала**		
	8	Семейство сетевых технологий Ethernet. Принцип работы Ethernet. Взаимодействие на подуровнях LLC и MAC. Управление доступом к среде передачи данных (CSMA). MAC-адрес: идентификация Ethernet. Атрибуты кадра Ethernet. Представления MAC-адресов. Одно- и многоадресной, широковещательной рассылок. Сквозное подключение, MAC- и IP-адреса.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.9. Протокол разрешения адресов (ARP)		**Содержание учебного материала**		
	9	Протокол разрешения адресов (ARP): принципы работы, роль в процессе удаленного обмена данными. Таблицы ARP на сетевых устройствах. Основные недостатки протокола ARP - Нагрузка на среду передачи данных и безопасность.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.10. Коммутатор		**Содержание учебного материала**		
	10	Основная информация о портах коммутатора. Таблица MAC-адресов коммутатора. Функция Auto-MDIX. Буферизация памяти на коммутаторах. Фиксированная и модульная конфигурации коммутаторов. Сравнение коммутации уровня 2 и уровня. Способы пересылки кадра на коммутаторах Cisco. Технология Cisco Express Forwarding. Виртуальный интерфейс коммутатора (SVI), Маршрутизируемый порт, EtherChannel уровня 3. Конфигурация маршрутизируемого порта.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	11	ПЗ 1. Просмотр MAC-адресов сетевых устройств. Изучение кадров Ethernet с помощью программы Wireshark	*2*	*ОК 01 – ОК 11,*

				ПК 1.1 – ПК 1.5
Практическое занятие		**Содержание практического занятия**		
	12	ПЗ 2. Просмотр ARP с помощью программы Wireshark, интерфейсов командной строки Windows и IOS. Использование интерфейса командной строки IOS с таблицами MAC-адресов коммутатора.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	13	ПЗ 3. Составление карты сети Интернет с помощью утилит «ping» и «traceroute»	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	14	ПЗ 4. Создание сети. Установка сеанса консоли с сетевым оборудованием при помощи программы Tera Term	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	15	ПЗ 5. Настройка основных параметров коммутатора. Просмотр сетевого трафика с помощью программы Wireshark.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.11. Сетевой уровень		**Содержание учебного материала**		
	16	Сетевой уровень в процессе передачи данных. Протоколы сетевого уровня. Основные характеристики IP-протокола.Структура пакетов IPv4 и IPv6. Особенности и преимущества протокола Pv6. Методы маршрутизации узлов. Таблица маршрутизации узлов и маршрутизатора для протоколов IPv4 и IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.12. Маршрутизатор		**Содержание учебного материала**		
	17	Устройство маршрутизатора – Процессор, память, операционная система. Подключение к маршрутизатору через различные порты. Настройка исходных параметров, интерфейсов, шлюза по умолчанию и других характеристик маршрутизатора.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	18	ПЗ 6. Просмотр таблиц маршрутизации узлов. Изучение физических характеристик	*2*	*ОК 01 –*

		маршрутизатора.		*ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	19	ПЗ 7. Создание сети, состоящей из коммутатора и маршрутизатора.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.13. Транспортный уровень		**Содержание учебного материала**		
	20	Назначение и задачи транспортного уровня. Мультиплексирование сеансов связи. Описание и сравнение протоколов TCP и UDP – надежность и производительность, область применения. Адресация портов и сегментация TCP и UDP. Обмен данными по TCP. Процессы TCP сервера. Установление TCP-соединения и его завершение. Принципы «трёхстороннего рукопожатия» TCP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание учебного материала**		
	21	ПЗ 8. Наблюдение за процессом трёхстороннего «рукопожатия» TCP с помощью программы Wireshark	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание учебного материала**		
	22	ПЗ 9. Изучение захваченных данных DNS UDP с помощью программы Wireshark. Изучение захваченных пакетов FTP и TFTP с помощью программы Wireshark	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.14. Установление TCP-соединения. Надёжность и управление потоком TCP		**Содержание учебного материала**		
	23	Установление TCP-соединения и его завершение. Принципы «трёхстороннего рукопожатия» TCP.Надёжность и управление потоком TCP - Подтверждение получения сегментов, потеря данных и повторная передача, управление потоком. Обмен данными с использованием UDP. Процессы и запросы UDP-сервера, UDP-датаграммы, процессы UDP-клиента. Приложения, использующие UDP и TCP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.15. IP-адресация		**Содержание учебного материала**		
	24	Структура IPv4-адресов. Сетевая и узловая часть IP-адреса. Преобразование адресов между двоичным и десятеричным представлением. Маска подсети IPv4. Сетевой адрес, адрес узла и широковещательный адрес сети IPv4. Присвоение узлу	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

		статического и динамического IPv4-адреса. Многоадресная передача. Публичные и частные IPv4-адреса. IPv4-адреса специального назначения. Присвоение IP-адресов. Совместное использование протоколов IPv4 и IPv6: двойной стек, туннелирование, преобразование. Представление IPv6-адресов. Правила сокращения записи IPv6-адресов. Индивидуальный, групповой, произвольный типы IPv6-адресов.		*ПК 1.5*
Тема 1.16. ICMP-сервисы		**Содержание учебного материала**		
	25	Структуры локального и глобального индивидуальных IPv6-адресов. Статическая и динамическая конфигурации глобального индивидуального адреса. Процесс EUI-64 и случайно сгенерированный идентификатор интерфейса. ICMP-сервисы. Отличия для протоколов IPv4 и IPv6. Сообщения ICMPvI6 «Запрос к маршрутизатору», «Объявление от маршрутизатора», «Запрос соседнего узла» и «Объявление соседнего узла». Тестирование сети с помощью эхо-запросов. Трассировка маршрута. Время прохождения сигнала в прямом и обратном направлениях (RTT). Время жизни (TTL) IPv4 и предел переходов IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.17. IP-адресация		**Содержание учебного материала**		
	26	Сегментация IP-сетей. Обмен данными между подсетями. Планирование адресации в подсетях. Расчетные формулы для сегментации сети. Разбиение на подсети на основе требований узлов и сетей, в соответствии с требованиями сетей. Определение маски подсети. Разбиение на подсети с использованием маски переменной длины (VLSM). Базовая модель и назначение блоков адресов VLSM. Планирование адресации сети. Особенности проектирования IPv6-сети. Разбиение на подсети с использованием идентификатора интерфейса.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	27	ПЗ 10. Изучение калькуляторов подсетей. Расчёт подсетей IPv4.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	28	ПЗ 11. Разделение сетей с различными топологиями на подсети.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	29	ПЗ 12. Разработка и внедрение схемы адресации разделённой на подсети IPv4-сети;	*2*	*ОК 01 –*

				ОК 11, ПК 1.1 – ПК 1.5
Практическое занятие		**Содержание практического занятия**		
	30	ПЗ 13. Настройка адресации IPv6. Проверка адресации IPv4 и IPv6	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	31	ПЗ 14. Конвертация IPv4-адресов в двоичную систему счисления. Определение IPv4/IPv6-адресов	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	32	ПЗ 15. Настройка IPv6-адресов на сетевых устройствах	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	33	ПЗ 16. Тестирование сетевого подключения с помощью команд «ping» и «traceroute». Проверка задержек в передачи сетевых пакетов с помощью утилит «ping» и «traceroute».	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	34	ПЗ 17. Организация подсети по различным сценариям	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	35	ПЗ 18. Разработка и внедрение структуры адресации VLSM. Внедрение схемы адресации разделённой на подсети IPv6-сети	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.18.		**Содержание учебного материала**		

Уровень приложений, уровень представления, сеансовый уровень.	36	Уровень приложений, уровень представления и сеансовый уровень. Примеры распространенных приложений. Протоколы уровня приложений. Одноранговые сети (P2P). Модель типа «клиент-сервер». Обзор протоколов HTTP, HTTPS, SMTP, POP и IMAP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.19. DNS, DHCP, FTP, SMB		**Содержание учебного материала**		
	37	Служба доменных имён (DNS). Формат сообщений и иерархия DNS. Утилита «nslookup». Служба DHCP. Протокол передачи файлов (FTP). Протокол обмена блоками серверных сообщений (SMB). Концепции «Всеобъемлющий Интернет» BYOD. Доставка данных по конвергентным сетям.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	38	ПЗ 19. Изучение функции обмена файлами между одноранговыми устройствами определение преобразований PAT	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	39	ПЗ 20. Изучение правил работы DNS. Изучение протокола FTP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.20. Создание и настройка компьютерной сети		**Содержание учебного материала**		
	40	Планирование и создание небольшой компьютерной сети: определение ключевых факторов, выбор топологии и сетевых устройств, выбор и настройка протоколов, системы адресации. Меры по обеспечению безопасности сети. Уязвимости и сетевые атаки. Разведывательные атаки, Атаки доступа, Отказ в обслуживании (DoS-атаки). Резервное копирование, обновление и установка исправлений. Межсетевые экраны.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	41	ПЗ 21. Анализ подключения компьютеров к сети с помощью кабелей и беспроводных адаптеров	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	42	ПЗ 22. Определение сетевых устройств и каналов связи. Просмотр данных о беспроводных и проводных сетевых адаптерах	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

				ПК 1.5
Практическое занятие		**Содержание практического занятия**		
	43	ПЗ 23. Обжим сетевого кабеля	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.21. Безопасность сети		**Содержание учебного материала**		
	44	Аутентификация, авторизация и учёт. Включение протокола SSH. Резервное копирование и восстановление с помощью текстовых файлов, протокола TFTP, USB-накопителя. Файловые системы маршрутизаторов и коммутаторов. Встроенные службы маршрутизации. Поддержка беспроводных подключений. Настройка встроенного маршрутизатора.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	45	ПЗ 24. Доступ к сетевым устройствам по протоколу SSH. Использование интерфейса командной строки (CLI) для сбора сведений о сетевых устройствах	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	46	Анализ трафика одноадресной передачи, широковещательной и многоадресной рассылки (практическое занятие)	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	47	Управление файлами конфигурации маршрутизатора с помощью программы эмуляции терминала	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	48	Обеспечение безопасности сетевых устройств. Изучение процедур восстановления паролей.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	49	Использование калькулятора Windows в работе с сетевыми адресами	*2*	*ОК 01 –*

				ОК 11, ПК 1.1 – ПК 1.5
Тема 2.	**Принципы маршрутизации и коммутации**		***62/36 (0)***	
Тема 2.1. Введение в коммутируемые сети		**Содержание учебного материала**		
	50	Объединённые сети. Иерархия в коммутируемой сети. Роль коммутируемых сетей. Коммутируемая среда. Динамическое заполнение таблицы MAC-адресов коммутатора. Методы пересылки на коммутаторе. Коммутация с промежуточным хранением. Сквозная коммутация. Коммутационные домены. Снижение перегрузок сети.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.2. Основные концепции и настройка коммутации		**Содержание учебного материала**		
	51	Основные концепции и настройка коммутации. Первоначальная настройка коммутатора и восстановление после системного сбоя. Настройка доступа для базового управления коммутатором с IPv4. Дуплексная связь. Настройка портов коммутатора на физическом уровне. Функция автоматического определения типа кабеля (Auto-MDIX). Проверка настроек порта коммутатора. Поиск и устранение проблем на уровне доступа к сети.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	52	ПЗ 25.Настройка коммутатора: Базовая настройка коммутатора. Настройка параметров безопасности коммутатора.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.3. Безопасность коммутатора.		**Содержание учебного материала**		
	53	Безопасность коммутатора. Защищённый удалённый доступ. Настройка SSH. Распространённые угрозы безопасности: переполнение таблицы MAC-адресов, DHCP-спуфинг, использование уязвимостей протокола CDP, Атаки Telnet и др. Аудит и практические рекомендации по обеспечению безопасности сети. Безопасность порта коммутатора. Отслеживание DHCP сообщений. Функция безопасности порта. Виды защиты MAC-адресов. Режимы реагирования на нарушение безопасности. Проверка и настройка портов. Протокол сетевого времени (NTP).	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	54	ПЗ 26. Настройка безопасности коммутатора: Настройка протокола SSH; Настройка функции Switch Port Security;	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

		Поиск и устранение неполадок в системе безопасности портов коммутатора; Отработка комплексных практических навыков.		*ПК 1.5*
Тема 2.4. Виртуальные локальные сети (VLAN)		**Содержание учебного материала**		
	55	Виртуальные локальные сети (VLAN) – классификация и основные характеристики. Транки виртуальных сетей. Контроль широковещательных доменов в сетях VLAN. Тегирование кадров Ethernet для идентификации сети VLAN. Сети native VLAN и тегирование стандарта 802.1Q. Тегирование голосовой VLAN. Реализации виртуальной локальной сети. Назначение портов сетям VLAN. Настройка транковых каналов. Протокол динамического создания транкового канала (DTP). Поиск и устранение неполадок в виртуальных локальных сетях и транковых каналах. Проблемы с IP-адресацией сети VLAN. Несовпадения режимов транковой связи. Проектирование и обеспечение безопасности VLAN: hopping, спуфинг коммутатора, атака с двойным тегированием, Сеть PVLAN периметра. Практические рекомендации по проектированию виртуальной локальной сети.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	56	ПЗ 27.Конфигурация сетей VLAN: Конфигурация сетей VLAN и транковых каналов; Поиск и устранение неполадок в конфигурации VLAN; Реализация системы безопасности сети VLAN; Реализация сетей VLAN для сегментации сетей предприятий малого и среднего бизнеса.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.5. Концепция маршрутизации		**Содержание учебного материала**		
	57	Настройка маршрутизатора. Механизмы пересылки пакетов. Подключение и настройка устройств. Светодиодные индикаторы на маршрутизаторе. Активация и настройка IP-адресации. Проверка связности сетей с прямым подключением. Проверка настроек интерфейса. Фильтрация выходных данных команд «show». Коммутация пакетов между сетями. Функция коммутации маршрутизатора. Маршрутизация пакетов. Определение пути. Процесс принятия решения о пересылке пакетов. Выбор оптимального пути. Протоколы RIP, OSPF, EIGRP. Распределение нагрузки. Администрирование расстояние (AD) и надежность маршрута. Анализ таблиц маршрутизации – источник данных, принципы формирование возможности настройки. Записи таблицы маршрутизации для сетей с прямым подключением. Задание статических маршрутов. Протоколы динамической маршрутизации сетей IPv4 и IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Практическое занятие		**Содержание практического занятия**		
	58	ПЗ 28.Настройка маршрутизатора: Использование команды traceroute для обнаружения сети; Документирование сети; Настройка интерфейсов IPv4 и IPv6; Настройка и проверка небольшой сети; Исследование маршрутов с прямым подключением.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	59	ПЗ 29.Настройка маршрутизации: Составление схемы сети Интернет; Настройка базовых параметров маршрутизатора с помощью интерфейса командной строки (CLI) системы Cisco IOS; Настройка базовых параметров маршрутизатора с помощью CCP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.6. Маршрутизация между VLAN		**Содержание учебного материала**		
	60	Принципы работы маршрутизации между VLAN. Настройка маршрутизации на базе маршрутизаторов с несколькими физическими интерфейсами, с использованием конфигурации router-on-a-stick, через многоуровневый коммутатор. Проблемы маршрутизации между VLAN. Проверка конфигурации коммутатора и настроек маршрутизатора. Неполадки в работе интерфейса. Ошибки в IP-адресах и масках подсети. Настройка и работа коммутации на 3-м уровне. Маршрутизация между VLAN через виртуальные интерфейсы коммутатора, маршрутизируемые порты. Неполадки в настройках коммутатора 3-го уровня.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Консультация	61	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
		Экзамен	***6***	
		6 семестр	***48/26(0)***	
Практическое занятие		**Содержание практического занятия**		
	62	ПЗ 30. Маршрутизация между VLAN: Настройка маршрутизации между VLAN для каждого интерфейса; Настройка маршрутизации между VLAN на основе стандарта 802.1Q и транкового канала; Поиск и устранение неполадок в маршрутизации между сетями VLAN.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Тема 2.7. Статическая маршрутизация		**Содержание учебного материала**		
	63	Преимущества и задачи статической маршрутизации. Типы статических маршрутов: стандартный, по умолчанию, суммарный, плавающий. Настройка статических маршрутов IPv4 и IPv6. Команда «ip route». Маршрут следующего перехода. Напрямую подключённый статический маршрут. Полностью заданный статический маршрут. Настройка статического маршрута по умолчанию. Классовая адресация. Классовые маски подсети. Бесклассовая междоменная маршрутизация CIDR. Объединение маршрутов. Организация суперсетей. Использование масок подсети фиксированной длины (FLSM). Маска подсети переменной длины (VLSM). Настройка суммарных и плавающих статических маршрутов. Расчёт суммарного маршрута. Объединение сетевых адресов IPv4 и IPv6. Поиск и устранение неполадок в настройках статического маршрута и маршрута по умолчанию.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	64	ПЗ 31. Настройка статической маршрутизации: Настройка статических маршрутов IPv4/IPv6 по умолчанию; Разработка и реализация схемы адресации IPv4 с использованием VLSM; Расчёт суммарных маршрутов IPv4 и IPv6; Поиск и устранение неполадок статических маршрутов IPv4 и IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.8. Динамическая маршрутизация		**Содержание учебного материала**		
	65	Протоколы динамической маршрутизации – назначение, принципы работы и история развития. Сравнение динамической и статической маршрутизации. Принципы работы протоколов маршрутизации: пуск после включения питания, Сетевое обнаружение, Обмен данными маршрутизации, Обеспечение сходимости. Классификация протоколов маршрутизации. Протоколы IGP и EGP. Дистанционно-векторные протоколы RIP, IGRP. Протоколы маршрутизации по состоянию канала OSPF и IS-IS. Классовые и бесклассовые протоколы маршрутизации. Характеристики и метрики протоколов.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	66	ПЗ 32. Настройка динамической маршрутизации: Исследование сходимости; Сравнение методов выбора пути в протоколах RIP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	67	ПЗ 33. Настройка протоколов RIPv2 и RIPng.	*2*	*ОК 01 –*

				ОК 11, ПК 1.1 – ПК 1.5
Тема 2.9. Динамическая дистанционно-векторная маршрутизация.		**Содержание учебного материала**		
	68	Динамическая дистанционно-векторная маршрутизация. Дистанционно-векторный алгоритм. Механизмы отправки и получения данных маршрутизации, расчёта оптимальных путей и добавления маршрутов в таблицу маршрутизации, обнаружения и реагирования на изменения в топологии. Настройка протокола RIP: включение RIPv2, отключение автоматического объединения, настройка пассивных интерфейсов, передача маршрута по умолчанию по сети. Настройка протокола RIPng. Процесс маршрутизации по состоянию канала. Hello протокол. пакет состояния канала (LSP). Лавинная рассылка пакетов состояния канала. Лавинная рассылка пакетов состояния канала. Создание дерева кратчайших путей SPF. Добавление маршрутов OSPF в таблицу маршрутизации. Недостатки протоколов маршрутизации по состоянию канала. Таблица маршрутизации. Записи с прямым подключением и удалённой сети. Динамически получаемые маршруты IPv4/6. Процесс поиска маршрута.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.10. OSPF для одной области		**Содержание учебного материала**		
	69	Семейство протоколов OSPF. Характеристики, принципы работы и компоненты OSPF. Особенности OSPF для одной и нескольких областей. Магистральная область. Инкапсуляция сообщений OSPF. Типы пакетов OSPF: пакет приветствия (hello), пакет описания базы данных (DBD), пакет запроса состояния канала (LSR), пакет обновления состояния канала (LSU). пакет подтверждения состояния канала (LSAck). Обновления состояния канала. Рабочие состояния OSPF. Выделенный (DR) и резервный выделенный маршрутизатор (BDR). Синхронизация баз данных OSPF. Настройка OSPFv2 для одной области. Режим конфигурации идентификаторы маршрутизатора. Использование интерфейса loopback. Включение OSPF на интерфейсах. Шаблонная маска. Команда «network». Настройка пассивных интерфейсов. Формула расчёта метрики стоимости OSPF. Настройка значений пропускной способности интерфейса. Проверка соседних устройств, настроек протокола, данных процесса и других характеристик OSPF. Сравнение OSPFv2 и OSPFv3. Адреса типа link-local. Топология сети OSPFv3. Настройка идентификатора маршрутизатора OSPFv3. Включение OSPFv3 на интерфейсах.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		

	70	ПЗ 34. Настройка протоколов OSPF: Настройка базового протокола OSPFv2 для одной области; Базовая настройка протокола OSPFv3 для одной области.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.11. Списки контроля доступа (ACL)		**Содержание учебного материала**		
	71	Списки контроля доступа (ACL). Принцип работы ACLсписков. Типы ACL-списков Cisco для IPv4. Присваивание номеров и имён ACL-спискам. Расчёт шаблонной маски в ACL-списках. Рекомендации по созданию и размещению ACL-списков. Размещение стандартных и расширенных ACL-списков. Настройка стандартного ACL-списка. Применение стандартных ACL-списков на интерфейсах. Комментарии к ACL-спискам. Проверка и редактирование стандартных нумерованных ACLсписков. ACL-статистика. Защита портов VTY с помощью стандартного ACL-списка IPv4. Структура и настройка расширенных ACL-списков для IPv4. Фильтрация трафика с использованием расширенных ACL-списков. Поиск и устранение неполадок ACL-списков. Распространённые ошибки ACL-списков. Сравнение ACL-списков для IPv4 и IPv6. Настройка и проверка ACL-списков для IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	72	ПЗ 35. Изучение механизмов работы со списками контроля доступа: Наглядное представление работы ACL-списка; Настройка стандартных ACL-списков; Настройка стандартных именованных ACL-списков; Настройка ACL-списка для линий VTY; Настройка расширенных ACL-списков для различных сценариев; Поиск и устранение неполадок в работе ACL-списков; Настройка ACL-списков IPv6; Отработка комплексных практических навыков.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	73	ПЗ 36. Настройка ACL-списков: Настройка и проверка стандартных ACL-списков; Настройка и проверка ограничений VTY; Настройка и проверка расширенных ACL-списков; Поиск и устранение неполадок в настройке и размещении ACL-списков; Настройка и проверка ACL-списков для IPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.12.		**Содержание учебного материала**		

Протокол DHCP	74	Протокол DHCP. DHCPv4: базовая операция, формат сообщений, сообщения обнаружения и предложения. Настройка, проверка и ретрансляция простого DHCPv4-сервера. Настройка маршрутизатора в качестве DHCPv4-клиента. Настройка маршрутизатора класса SOHO. Поиск и устранение неполадок в работе маршрутизатора DHCPv4. Протокол DHCPv6. Автоматическая настройка адреса без отслеживания состояния (SLAAC). Принцип работы SLAAC с DHCPv6. DHCPv6 с и без отслеживания состояния. Процессы DHCPv6. Настройка маршрутизатора в качестве DHCPv6-сервера и DHCPv6-клиента. Поиск и устранение неполадок в работе DHCPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	75	ПЗ 37. Изучение протоколов DHCP: Базовая настройка DHCPv4 на маршрутизаторе; Базовая настройка DHCPv4 на коммутаторе;	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	76	ПЗ 38. Поиск и устранение неполадок в работе DHCPv4; Настройка сервера DHCPv6 без отслеживания состояния и с отслеживанием состояния; Поиск и устранение неполадок в работе DHCPv6.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	77	ПЗ 39. Изучение протокола DHCP: Настройка протокола DHCP с помощью команд Cisco IOS; Отработка комплексных практических навыков.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.13. Преобразование сетевых адресов IPv4		**Содержание учебного материала**		
	78	Преобразование сетевых адресов IPv4. Концептуальное преобразование сетевых адресов (NAT). Терминология и принципы работы NAT. Пространство частных IPv4-адресов. Статическое и динамическое преобразование сетевых адресов (NAT). Преобразование адресов портов (PAT). Сравнение NAT и PAT. Преимущества и недостатки NAT. Анализ статического преобразования NAT. Принцип работы динамического NAT Настройка и проверка NAT, PAT. Переадресация портов. Настройка NAT и протокола IPv6. Поиск и устранение неполадок в работе NAT.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	79	ПЗ 40. Преобразование сетевых адресов:	*2*	*ОК 01 –*

		Изучение принципа работы NAT; Настройка статического и динамического NAT; Реализация статического и динамического NAT;		*ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	80	ПЗ 41. Настройка переадресации портов на маршрутизаторе Linksys; Проверка, поиск и устранение неполадок конфигураций NAT; Отработка комплексных практических навыков.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	81	ПЗ 42. Изучение работы с NAT и PAT: Настройка динамического и статического NAT; Настройка NAT-пула с перегрузкой и PAT; Поиск и устранение неполадок конфигураций NAT.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Консультация	82	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
		Экзамен	*6*	

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа**		**Объем часов**	**Коды компетенций**
1	**2**		**3**	**4**
МДК.01.02	**Организация, принципы построения и функционирования компьютерных сетей**		***175/90(15)***	
	5 семестр		***117/80(9)***	
Тема 1.	**Маршрутизация и коммутация. Масштабирование сетей.**		***64/48(4)***	
Тема 1.1. Введение в масштабирование сетей		**Содержание учебного материала**		
	1	Реализация проекта сети. Проект иерархической сети. Расширение сети. Выбор сетевых устройств. Коммутационное оборудование. Маршрутизаторы. Управляющие устройства.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Практическое занятие		**Содержание практического занятия**		
	2	ПЗ 1. Развертывание коммутируемой сети с резервными каналами	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.2. Избыточность LAN		**Содержание учебного материала**		
	3	Понятия протокола spanning-tree. Предназначение протокола spanning-tree. Принцип работы STP. Типы протоколов STP. Настройка протокола STP. Настройка PVST+. Настройка Rapid PVST+. Проблемы настройки STP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	4	ПЗ 2. Настройка Rapid PVST+, PortFast и BPDU Guard	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	5	ПЗ 3. Настройка PortFast и BPDU Guard	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	6	ПЗ 4. Настройка BPDU Guard	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.3. Агрегирование каналов		**Содержание учебного материала**		
	7	Основные понятия агрегирования каналов. Агрегирование каналов. Принцип работы EtherChannel. Настройка агрегирования каналов. Настройка EtherChannel. Проверка, поиск и устранение неполадок в работе EtherChannel	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	8	ПЗ 5. Настройка протокола GLBP	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

				ПК 1.5
Практическое занятие		**Содержание практического занятия**		
	9	ПЗ 6. Определение типовых ошибок конфигурации STP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	10	ПЗ 7. Определение типовых ошибок конфигурации STP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	11	ПЗ 8. Настройка EtherChannel	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	12	ПЗ 9. Поиск и устранение неполадок в работе EtherChannel	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	13	ПЗ 10. Агрегирование каналов	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	14	ПЗ 11. Агрегирование каналов	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	15	Систематическая проработка конспектов занятий, учебной и специальной технической литературы.	*2*	*ОК 01 – ОК 11,*

				ПК 1.1 – ПК 1.5
Самостоятельная работа		**Содержание самостоятельной работы**		
	16	Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.4. Беспроводные локальные сети		**Содержание учебного материала**		
	17	Концепции беспроводной связи. Введение в беспроводную связь. Компоненты сетей WLAN. Топологии сетей WLAN 802.11. Принципы работы беспроводной локальной сети. Структура кадра 802.11. Функционирование беспроводной связи. Управление каналами. Безопасность беспроводных локальных сетей. Угрозы для сетей WLAN. Обеспечение безопасности WLAN. Настройка беспроводных локальных сетей. Настройка беспроводного маршрутизатора. Настройка беспроводных клиентов. Поиск и устранение неполадок в работе сетей WLAN.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	18	ПЗ 12. Настройка беспроводного маршрутизатора и клиента	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	19	ПЗ 13. Настройка беспроводного маршрутизатора и клиента	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 1.5. Настройка и устранение неполадок в работе OSPF для одной области		**Содержание учебного материала**		
	20	Расширенные параметры протокола OSPF для одной области. Маршрутизация на уровнях распределения и ядра. OSPF в сетях с множественным доступом. Распространение маршрута по умолчанию. Точная настройка интерфейсов OSPF. Защита OSPF. Устранение неполадок реализации протокола OSPF для одной области. Составляющие процедуры поиска и устранения неполадок в работе OSPF для одной области. Поиск и устранение неполадок в маршрутизации OSPFv2 для одной области. Поиск и устранение неполадок в OSPFv3 для одной области	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		

	21	ПЗ 14. Настройка базового протокола OSPFv2 для одной области	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	22	ПЗ 15. Настройка OSPFv2 в сети множественного доступа	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	23	ПЗ 16. Настройка расширенных функций OSPFv2	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	24	ПЗ 17. Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	25	ПЗ 18. Поиск и устранение неполадок в работе основных протоколов OSPFv2 и OSPFv3 для одной области	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	26	ПЗ 19. Поиск и устранение неполадок в работе усовершенствованного протокола OSPFv2 для одной области	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	27	ПЗ 20. Владение навыками поиска и устранения неполадок в работе OSPF	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Тема 1.6. OSPF для нескольких областей		**Содержание учебного материала**		
	28	Принцип работы OSPF для нескольких областей. Назначение OSPF для нескольких областей. Принцип работы пакетов LSA в OSPF для нескольких областей. Таблица маршрутизации и типы маршрутов OSPF. Настройка OSPF для нескольких областей. Настройка OSPF для нескольких областей. Объединение маршрутов OSPF. Проверка OSPF для нескольких областей.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	29	ПЗ 21. Настройка OSPFv2 для нескольких областей	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	30	ПЗ 22. Настройка OSPFv3 для нескольких областей	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	31	ПЗ 23. Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	32	ПЗ 24. Поиск и устранение неполадок в работе OSPFv2 и OSPFv3 для нескольких областей	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.	**Соединение сетей**		***93/42(11)***	
Самостоятельная работа		**Содержание самостоятельной работы**		
	33	**Подключение к глобальной сети** Обзор технологий глобальной сети. Цель создания глобальных сетей. Принцип работы глобальной сети. Выбор технологии глобальной сети. Сервисы глобальной сети. Инфраструктуры частных глобальных сетей. Инфраструктура общедоступной глобальной сети. Выбор сервисов глобальной сети.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		

	34	Подготовка к лабораторным и практическим работам с использованием методических рекомендаций преподавателя, оформление лабораторно-практических работ, отчётов и подготовка к их защите.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.1. Соединение «точка-точка»		**Содержание учебного материала**		
	35	Обзор последовательного соединения «точка-точка». Связь по последовательному каналу. Инкапсуляция HDLC. Принцип работы протокола PPP. Преимущества протокола PPP. LCP и NCP. Сеансы PPP. Настройка протокола PPP. Настройка протокола PPP. Аутентификация PPP. Отладка соединений WAN. Отладка PPP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	36	ПЗ 25. Настройка базового PPP с аутентификацией	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	37	ПЗ 26. Отладка базового PPP с аутентификацией	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	38	ПЗ 27. Отладка базового PPP с аутентификацией	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	39	ПЗ 28. Проверка PPP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.2. Решения широкополосного доступа		**Содержание учебного материала**		
	40	Удалённая работа. Преимущества удалённой работы. Бизнес-требования для удалённых работников. Сравнение решений широкополосного доступа. Кабель. DSL. Беспроводные широкополосные сети. Выбор решений широкополосного доступа. Настройка подключений xDSL. Обзор PPPoE. Настройка PPPoE.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Практическое занятие		**Содержание практического занятия**		
	41	ПЗ 29. Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	42	ПЗ 30. Настройка маршрутизатора в качестве клиента PPPoE для подключения DSL	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.3. Защита межфилиальной связи		**Содержание учебного материала**		
	43	Сети VPN. Основы сетей VPN. Типы сетей VPN. Туннели GRE между объектами. Основы GRE. Настройка туннелей GRE. Общие сведения об IPsec. Защита протокола IP. Структура протокола IPsec. Удалённый доступ. Решения VPN для удалённого доступа. Сети VPN удалённого доступа с использованием IPsec.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	44	ПЗ 31. Настройка туннеля VPN GRE по схеме «точка-точка»	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	45	ПЗ 32. Разработка технического обслуживания сети	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	46	ПЗ 33. Разработка технического обслуживания сети	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Тема 2.4. Мониторинг Сети		**Содержание учебного материала**		
	47	Syslog. Принцип работы Syslog. Настройка Syslog. SNMP. Принцип работы SNMP. Настройка SNMP. NetFlow. Принцип работы NetFlow. Настройка NetFlow. Проверка моделей трафика.	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

				ПК 1.5
Практическое занятие		**Содержание практического занятия**		
	48	ПЗ 34. Настройка Syslog и NTP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	49	ПЗ 35. Настройка NTP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	50	ПЗ 36. Принцип работы SNMP. Настройка SNMP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	51	ПЗ 37. Принцип работы NetFlow. Настройка NetFlow.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	52	ПЗ 38. Изучение программного обеспечения для мониторинга сети	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	53	ПЗ 39. Настройка SNMP	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	54	ПЗ 40. Сбор и анализ данных NetFlow	*2*	*ОК 01 – ОК 11,*

				ПК 1.1 – ПК 1.5
Самостоятельная работа		**Содержание самостоятельной работы**		
	55	Оформление лабораторно-практических работ, отчётов и подготовка к их защите.	*1*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Консультация	56	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
		Экзамен	***6***	
6 семестр			***58/10(6)***	
Тема 2.5. Отладка сети		**Содержание учебного материала**		
	57	Поиск и устранение неполадок с использованием системного подхода. Документация по сети. Процедура поиска и устранения неполадок. Изоляция проблемы с помощью многоуровневых моделей. Отладка сети. Средства поиска и устранения неполадок. Симптомы и причины отладки сети. Поиск и устранение неполадок связи в сетях IP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	58	ПЗ 41. Инструментарий сетевого администратора для наблюдения	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	59	ПЗ 42. Инструментарий сетевого администратора для наблюдения	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	60	ПЗ 43. Сбой в работе сети	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		

	61	ПЗ 44. Поиск и устранение неполадок связи в сетях IP.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Практическое занятие		**Содержание практического занятия**		
	62	ПЗ 45. Разработка документации КС	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Консультация	63	Повторение и обобщение изученного материала. Подготовка к курсовой работе.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	64	Выбор темы курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	65	Подбор, изучение, анализ литературы по выбранной теме	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	66	Отбор фактического материала по выбранной теме	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	67	Отбор фактического материала по выбранной теме	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		

	68	Требования к структуре курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	69	Требования к содержанию курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	70	Составление плана курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	71	Написание введения и заключения курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	72	Стиль изложения научных материалов	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	73	Технические требования к оформлению	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	74	Технические требования к оформлению	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*

Курсовая работа		**Содержание материала**		
	75	Рецензирование курсовых работ	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	76	Подготовка речи к выступлению	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	77	Защита курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Курсовая работа		**Содержание материала**		
	78	Защита курсовой работы	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	79	Оформление лабораторно-практических работ, отчётов и подготовка к их защите.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	80	Оформление лабораторно-практических работ, отчётов и подготовка к их защите.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
Самостоятельная работа		**Содержание самостоятельной работы**		
	81	Построение и настройка ЛКС	*2*	*ОК 01 – ОК 11, ПК 1.1 –*

				ПК 1.5
Консультация	82	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
		Экзамен	***6***	
Учебная практика		**Виды работ**	***216***	
	1	Проектирование общей топологии	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	2	Проектирование физической топологии	*6*	
	3	Проектирование физической топологии	*6*	
	4	Проектирование логической топологии	*6*	
	5	Настройка виртуального стенда	*6*	
	6	Настройка виртуального стенда	*6*	
	7	Документирование сети	*6*	
	8	Обжим прямого и перекрёстного кабеля	*6*	
	9	Обжим прямого и перекрёстного кабеля	*6*	
	10	Монтаж сетевых розеток	*6*	
	11	Монтаж сетевых розеток	*6*	
	12	Монтаж коммуникационной панели	*6*	
	13	Монтаж коммуникационной панели	*6*	
	14	Принципы передачи сигналов по оптическому волокну	*6*	
	15	Структурная схема построения ВОЛС. Классификация сетей	*6*	
	16	Сварка волоконно-оптического кабеля	*6*	
	17	Оптические защитные муфты, классификация и характеристики.	*6*	
	18	Монтаж и демонтаж оптических муфт	*6*	
	19	Монтаж и демонтаж оптических муфт	*6*	
	20	Измерение затухания на смонтированных линиях с помощью оптического тестера	*6*	
	21	Структурированные кабельные системы	*6*	
	22	Базовая настройка сетевого коммутатора	*6*	
	23	Базовая настройка сетевого коммутатора	*6*	
	24	Изучение ARP-таблицы	*6*	
	25	Базовая настройка корпоративного маршрутизатора.	*6*	
	26	Базовая настройка корпоративного маршрутизатора.	*6*	

	27	Настройка IPv6 на сетевых устройствах.	*6*	
	28	Расчёт подсетей IPv4	*6*	
	29	Разработка и внедрение схемы адресации IPv4 и IPv6.	*6*	
	30	Разработка и реализация схемы адресации VLSM	*6*	
	31	Исследование процесса трёхстороннего квитирования протокола TCP	*6*	
	32	Настройка беспроводного маршрутизатора.	*6*	
	33	Настройка протокола SSH. Просмотр таблиц маршрутизации узлов.	*6*	
	34	Сравнение и анализ таблиц маршрутизации узлов	*6*	
	35	Определение сетевого адреса. Расчет количества допустимых узлов (базовый уровень)	*6*	
	36	Определение допустимых адресов узлов. Расчет маски подсети (базовый уровень).	*6*	
Производственная практика		**Виды работ**	***216***	
	Участие в управлении сетевыми сервисами			
	1	Взаимодействие клиента и сервера	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	2	Роль протоколов	*6*	
	3	Транспортные протоколы	*6*	
	4	Прикладные протоколы и службы	*6*	
	5	Служба доменных имен	*6*	
	6	Клиенты и серверы электронной почты	*6*	
	7	Ftp клиенты и серверы	*6*	
	8	Модель OSI	*6*	
	Участие в модернизации сетевой инфраструктуры			
	9	Сбор требований к сети	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	10	Выбор и конструирование сети	*6*	
	11	Реализация сети	*6*	
	12	Эксплуатация сети	*6*	
	13	Проверка и оценка сети	*6*	
	Сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей			
	14	Документирование характеристик существующей сети	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	15	Осмотр сети	*6*	
	16	Физическая топология	*6*	
	17	Логическая топология	*6*	
	18	Документирование сетевых требований	*6*	

	Проведение профилактических работ на объектах сетевой инфраструктуры и рабочих станциях			
	19	Шифрование данных на жестких дисках серверов	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	20	Разграничение доступа к файлам	*6*	
	21	Сканирование системы безопасности	*6*	
	22	Управления обновлением ПО	*6*	
	23	Разделение прав пользователей, которым разрешен доступ	*6*	
	Участие в инвентаризации технических средств сетевой инфраструктуры, осуществление контроля поступившего из ремонта оборудования			
	24	Инвентаризация сетевого оборудования	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	25	Методы резервного копирования	*6*	
	26	Диагностика оборудования	*6*	
	27	Диагностика оборудования	*6*	
	Замена расходных материалов и мелкий ремонт периферийного оборудования, определение устаревшего оборудования и программных средств сетевой инфраструктуры			
	28	Замена расходных материалов	*6*	*ОК 01 – ОК 11, ПК 1.1 – ПК 1.5*
	29	Замена расходных материалов	*6*	
	30	Мелкий ремонт периферийного оборудования	*6*	
	31	Мелкий ремонт периферийного оборудования	*6*	
	32	Определение устаревшего оборудования	*6*	
	33	Определение устаревшего оборудования	*6*	
	34	Обновление сетевого оборудования	*6*	
	35	Обновление сетевого оборудования	*6*	
	36	Обновление сетевого оборудования	*6*	
		Квалификационный экзамен	***18***	
		Всего:	***801/174(23)***	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля требует наличия следующих специальных помещений:

Лаборатория «Организация и принципы построения компьютерных систем», оснащенная в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

Для выполнения практических лабораторных занятий курса в группах (до 15 человек) требуются компьютеры и периферийное оборудование в приведенной ниже конфигурации:

– 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, лицензионный 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, FRC 2068 — HTTP,

RFC 2131 — DHCP, RFC 2138 — RADIUS, RFC 2233 - IF MIB v3, RFC 2373 - IPv6 Aggrega-table 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.

Студия «Проектирования и дизайна сетевых архитектур и инженерной графики», оснащенная в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

– Автоматизированные рабочие места на 12-15 обучающихся с конфигурацией: Core i3 или аналог, дискретная видеокарта, не менее 8GB ОЗУ, один или два монитора 23", мышь, клавиатура;

– Автоматизированное рабочее место преподавателя с конфигурацией: Core i5 или аналог, дискретная видеокарта, не менее 8GB ОЗУ, один или два монитора 23", мышь, клавиатура;

– Специализированная эргономичная мебель для работы за компьютером;

– Офисный мольберт (флипчарт);

– Проектор и экран;

– Маркерная доска;

– Принтер А3, цветной;

– Программное обеспечение общего и профессионального назначения.

Оснащенные базы практики, в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Н.В. Максимов, И.И. Попов. Компьютерные сети [Электронный ресурс]: учеб. Пособие -М.: ФОРУМ: ИНФРА-М 2017.
2. Новожилов Е.О. Компьютерные сети.–М.: ОИЦ «Академия, 2017.

Интернет ресурсы:

3. Гарант. Информационно-правовой портал [Электронный ресурс] : сайт. – Режим доступа: http://www.garant.ru.
4. Электронно-библиотечная система BOOK.ru [Электронный ресурс]: сайт. – Режим доступа: http://www.book.ru.
5. Российская государственная библиотека [Электронный ресурс] / Центр информ. Технологий РГБ ; ред. Власенко Т.В. ; Web-мастер Козлова Н.В. – Электрон.дан. – М. : Рос.гос. б-ка. – Режим доступа: http://www.rsl.ru.

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

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	**Критерии оценки**	**Методы оценки**
ПК 1.1. Выполнять проектирование кабельной структуры компьютерной сети.	Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» - алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 1. 2. Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности.	Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

ПК 1. 3. Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.	Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 1. 4. Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.	Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 1. 5. Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.	Оценка «отлично» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «хорошо» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «удовлетворительно» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОП 02.Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности для решения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.	- эффективно использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 09. Использовать информационные технологии в профессиональной деятельности.	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный

ОК 10. Пользоваться профессиональной документацией на государственном и иностранном языке.	- эффективность использования в профессиональной деятельности необходимой технической документации, в том числе на английском языке.	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере.	- эффективно планировать предпринимательскую деятельность в профессиональной сфере при проведении работ по конструированию сетевой инфраструктуры	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный

ПМ 01. Выполнение работ по проектированию сетевой инфраструктуры

Календарный план по учебной практике

№ п/п	Содержание	Кол-во часов/дней	Примечание
1	Проектирование общей топологии	**6/1**	
2	Проектирование физической топологии	**6/1**	
3	Проектирование физической топологии	**6/1**	
4	Проектирование логической топологии	**6/1**	
5	Настройка виртуального стенда	**6/1**	
6	Настройка виртуального стенда	**6/1**	
7	Документирование сети	**6/1**	
8	Обжим прямого и перекрёстного кабеля	**6/1**	
9	Обжим прямого и перекрёстного кабеля	**6/1**	
10	Монтаж сетевых розеток	**6/1**	
11	Монтаж сетевых розеток	**6/1**	
12	Монтаж коммуникационной панели	**6/1**	
13	Монтаж коммуникационной панели	**6/1**	
14	Принципы передачи сигналов по оптическому волокну	**6/1**	
15	Структурная схема построения ВОЛС. Классификация сетей	**6/1**	
16	Сварка волоконно-оптического кабеля	**6/1**	
17	Оптические защитные муфты, классификация и характеристики.	**6/1**	
18	Монтаж и демонтаж оптических муфт	**6/1**	
19	Монтаж и демонтаж оптических муфт	**6/1**	
20	Измерение затухания на смонтированных линиях с помощью оптического тестера	**6/1**	
21	Структурированные кабельные системы	**6/1**	
22	Базовая настройка сетевого коммутатора	**6/1**	
23	Базовая настройка сетевого коммутатора	**6/1**	
24	Изучение ARP-таблицы	**6/1**	
25	Базовая настройка корпоративного маршрутизатора.	**6/1**	
26	Базовая настройка корпоративного маршрутизатора.	**6/1**	
27	Настройка IPv6 на сетевых устройствах.	**6/1**	
28	Расчёт подсетей IPv4	**6/1**	
29	Разработка и внедрение схемы адресации IPv4 и IPv6.	**6/1**	
30	Разработка и реализация схемы адресации VLSM	**6/1**	
31	Исследование процесса трёхстороннего	**6/1**	

	квитирования протокола TCP		
32	Настройка беспроводного маршрутизатора.	**6/1**	
33	Настройка протокола SSH. Просмотр таблиц маршрутизации узлов.	**6/1**	
34	Сравнение и анализ таблиц маршрутизации узлов	**6/1**	
35	Определение сетевого адреса. Расчет количества допустимых узлов (базовый уровень)	**6/1**	
36	Определение допустимых адресов узлов. Расчет маски подсети (базовый уровень).	**6/1**	
	ИТОГО	**216/36**	

Календарный план по производственной практике (по профилю специальности)

№ п/п	Содержание	Кол-во часов/дней	Примечание
1	Взаимодействие клиента и сервера	**6/1**	
2	Роль протоколов	**6/1**	
3	Транспортные протоколы	**6/1**	
4	Прикладные протоколы и службы	**6/1**	
5	Служба доменных имен	**6/1**	
6	Клиенты и серверы электронной почты	**6/1**	
7	Ftp клиенты и серверы	**6/1**	
8	Модель OSI	**6/1**	
9	Сбор требований к сети	**6/1**	
10	Выбор и конструирование сети	**6/1**	
11	Реализация сети	**6/1**	
12	Эксплуатация сети	**6/1**	
13	Проверка и оценка сети	**6/1**	
14	Документирование характеристик существующей сети	**6/1**	
15	Осмотр сети	**6/1**	
16	Физическая топология	**6/1**	
17	Логическая топология	**6/1**	
18	Документирование сетевых требований	**6/1**	
19	Шифрование данных на жестких дисках серверов	**6/1**	
20	Разграничение доступа к файлам	**6/1**	
21	Сканирование системы безопасности	**6/1**	
22	Управления обновлением ПО	**6/1**	
23	Разделение прав пользователей, которым разрешен доступ	**6/1**	
24	Инвентаризация сетевого	**6/1**	

	оборудования		
25	Методы резервного копирования	**6/1**	
26	Диагностика оборудования	**6/1**	
27	Диагностика оборудования	**6/1**	
28	Замена расходных материалов	**6/1**	
29	Замена расходных материалов	**6/1**	
30	Мелкий ремонт периферийного оборудования	**6/1**	
31	Мелкий ремонт периферийного оборудования	**6/1**	
32	Определение устаревшего оборудования	**6/1**	
33	Определение устаревшего оборудования	**6/1**	
34	Обновление сетевого оборудования	**6/1**	
35	Обновление сетевого оборудования	**6/1**	
36	Обновление сетевого оборудования	**6/1**	
	ИТОГО	**216/36**	

Вид промежуточной аттестации: дифференцированный зачёт

Приложение 1А

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПМ.01. Выполнение работ по проектированию сетевой инфраструктуры

Специальность: 09.02.06 Сетевое и системное администрирование

Содержание

1. Пояснительная записка

Фонд оценочных средств по профессиональному модулю ПМ.01. Выполнение работ по проектированию сетевой инфраструктуры разработан на основании требований ФГОС СПО, с учетом профессиональной направленности программ среднего профессионального образования.

Основная цель создания фонда оценочных средств профессионального модуля – совершенствование содержания профессионального модуля для формирования профессионально-значимых компетенций. Фонд оценочных средств представлен комплектом контрольно-оценочных средств.

ФОС состоит из оценочных средств для: текущего контроля, рубежного контроля и промежуточной аттестации обучающихся.

2.Описание контрольно-оценочных средств

Фонд оценочных средств для текущего, рубежного контроля и промежуточной аттестации разработан для оценки уровня освоения обучающимися планируемых результатов. В ФОС раскрыта типология оценочных ситуаций и заданий текущего, рубежного контроля и промежуточной аттестации, по итогам освоения разделов основного содержания профессионального модуля.

Структурные элементы ФОС по профессиональному модулю:

- результаты освоения ПМ, подлежащие проверке;
- описание контрольно-оценочных средств;
- разноформатные задания для текущего контроля по ПМ;
- разноформатные задания для рубежного контроля по ПМ;
- разноформатные задания для промежуточной аттестации по ПМ.

Кроме оценочных заданий, ФОС включает эталоны ответов к некоторым заданиям, а к типовым – алгоритмы решения либо ориентировочную основу действий.

2.1 Планируемые результаты освоения профессионального модуля

Планируемые результаты освоения профессионального модуля в соответствии с ФГОС СПО

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 традиционных 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 поддержание 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.

Код	Наименование видов деятельности и профессиональных компетенций
ВД 1.	Выполнение работ по проектированию сетевой инфраструктуры
ПК 1.1.	Выполнять проектирование кабельной структуры компьютерной сети.
ПК 1.2.	Осуществлять выбор технологии, инструментальных средств и средств вычислительной техники при организации процесса разработки и исследования объектов профессиональной деятельности
ПК 1.3.	Обеспечивать защиту информации в сети с использованием программно-аппаратных средств.
ПК 1.4.	Принимать участие в приемо-сдаточных испытаниях компьютерных сетей и сетевого оборудования различного уровня и в оценке качества и экономической эффективности сетевой топологии.
ПК 1.5.	Выполнять требования нормативно-технической документации, иметь опыт оформления проектной документации.

3.Фонды оценочных средств
3.1 Фонд оценочных средств для текущего контроля

Текущий контроль проводится во время аудиторных занятий по ПМ.01. Выполнение работ по проектированию сетевой инфраструктуры в соответствии с учебным планом и рабочей программой ПМ.01. Выполнение работ по проектированию сетевой инфраструктуры.

Вариант 1

1. Компьютерная сеть — это группа устройств, объединенных между собой каким-либо способом с целью совместного доступа к ресурсам и обмена информацией.
а. верно
б. неверно

2. Как называется тип взаимодействия между компьютерами, при котором каждый из них может выступать как в роли сервера, так и в роли клиента
а. сеть типа «клиент-клиент»
б. сеть типа «клиент-сервер»

3. Какой из уровней модели OSI выполняет передачу потока битов через среду в виде электрических, оптических или радиосигналов?
а. сетевой уровень
б. физический уровень
в. канальный уровень

4. Виртуальная сеть – это
а. Компьютерная сеть, охватывающая большие территории и включающая в себя сети городов, стран, континентов
б. Группа узлов, связанных друг с другом и расположенных на небольшой территории
в. Сеть, получившаяся в результате объединения двух или нескольких территориально распределенных локальных сетей с помощью каналов глобальных сетей

5. Сетевой уровень модели OSI отвечает за_____адресацию
а. физическую
б. логическую

6. Для записи MAC-адреса используется точечно-десятичная нотация
а. верно
б. неверно

7. Что такое беспроводная сеть?
а. Сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне
б. Сеть, в которой для передачи данных используются металлические кабели (коаксиальный, витая пара) или волоконно-оптические кабели.

8. Сколько уровней в модели OSI? Введите число.
а. 6
б. 5
в. 8
г. 7

9. Для чего используется доменное имя?

а. для передачи файлов между клиентом и сервером
б. для установления соединения перед передачей данных
в. для уникальной буквенно-цифровой идентификации определенного узла, являющегося частью Интернета
г. для получения электронной почты с удаленного сервера

10. На каком уровне модели OSI взаимодействуют Web-браузеры с Web-серверами?
а. физическом уровне
б. уровне приложений
в. транспортном уровне
г. сеансовом уровне

Вариант 2

1. Выберите все, что можно отнести к сетям общего пользования
а. корпоративная сеть
б. локальная сеть
в. сеть Интернет
г. сеть радиовещания

2. MAC-адрес — это логический адрес
а. верно
б. неверно

3. Как называется тип взаимодействия между компьютерами, при котором каждый из них может выступать как в роли сервера, так и в роли клиента
а. сеть типа «клиент-клиент»
б. сеть типа «клиент-сервер»

г. одноранговая сеть

4. К уровню приложений модели TCP/IP относятся протоколы
а. HTTP, Telnet, FTP
б. TCP, UDP
в. Ethernet, PPP

5. Глобальная сеть – это
а. Сеть, получившаяся в результате объединения двух или нескольких территориально распределенных локальных сетей с помощью каналов глобальных сетей
б. Компьютерная сеть, связывающая множество локальных сетей на территории одного города
в. Компьютерная сеть, охватывающая большие территории и включающая в себя сети городов, стран, континентов

6. Для записи IP-адреса используется точечно-десятичная нотация
а. верно
б. неверно

7. Какой уровень модели OSI отвечает за передачу данных между локальными устройствами?
а. канальный
б. приложений
в. физический

8. Нижние уровни модели OSI (с 1 по 3) управляют физической доставкой данных по сети и реализуются в виде аппаратных средств и программного обеспечения
а. верно
б. неверно

9. Какой уровень модели OSI отвечает за выбор наилучшего маршрута до сети назначения и логическую адресацию?
а. физический уровень
б. сетевой уровень
в. уровень приложений

10. Компьютерная сеть, охватывающая большие территории и включающая в себя сети городов, стран, континентов

а. виртуальная сеть
б. сеть мегаполиса
в. глобальная сеть

Ключи к тесту

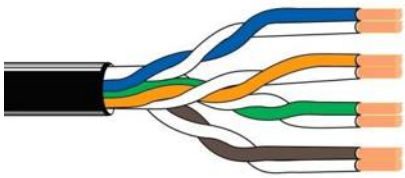
Вариант 1		Вариант 2	
№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	б	1	вг
2	б	2	б
3	б	3	г
4	в	4	а
5	б	5	в
6	б	6	а
7	а	7	а
8	г	8	а
9	в	9	б
10	б	10	в

Вариант 3.

1. IP-адрес - это
а. физический адрес
б. логический адрес

2. Выберите основную функцию четвёртого уровня модели OSI
а. Обеспечивает надёжную доставку сегментов по сети
б. Передаёт электрические сигналы между устройствами
в. Выполняет передачу данных между локальными устройствами
г. Выбирает наилучший маршрут до сети назначения

3. На рисунке представлен



а. волоконно-оптический кабель
б. кабель типа «витая пара»

4. Переведите IPv4-адрес 11101100 00010001 00001100 00001111 из двоичного вида в десятичный.
а. 192.168.1.182
б. 236.17.12.15
в. 236.18.10.14

5. Что такое беспроводная сеть?

а. Сеть, в которой передача информации осуществляется при помощи электромагнитных волн в определенном частотном диапазоне

б. Сеть, в которой для передачи данных используются металлические кабели (витая пара) или волоконно-оптические кабели

6. Выберите основную функцию четвёртого уровня модели OSI.

а. Обеспечивает надёжную доставку сегментов по сети
б. Передаёт электрические сигналы между устройствами
в. Выполняет передачу данных между локальными устройствами
г. Выбирает наилучший маршрут до сети назначения

7. Выберите все, что можно отнести к сетям общего пользования.
а. корпоративная сеть
б. локальная сеть
в. сеть Интернет
г. сеть радиовещания

8. По какой формуле определяется максимальное количество устройств, которые могут быть включены в IP-сеть?(n-число нулей в сетевой маске)
а. n^2
б. 2^n
в. n^2-2
г.2^n-2
д. 2^n-1

9. Дано:
Маскасети:255.255.255.248
АдресIP:192.168.1.219
Определите адрес сети
а. 192.168.1.0
б. 192.168.1.255
в. 192.168.1.216
г. 192.168.1.223
10. К недостаткам оптоволоконного кабеля относят:
а. плохая помехозащищенность
б. сложность ремонта
в. низкая скорость передачи данных
г. низкая секретность передаваемой информации

Вариант 4

1. Кто является активной стороной при установлении соединения?

а клиент и сервер
б. клиент
в сервер

2. Что определяется с помощью утилиты ping?
а. время задержки прохождения пакета до указанного узла
б. время задержки прохождения пакета до указанного узла и обратно
в путь до указанного узла
г путь до указанного узла и обратно

3. Провода витой пары скручивают для
а) более компактного размещения их в защитной оболочке
б) уменьшения помех, вызванных магнитными потоками
в) четкого разделения каждой пары проводов
г) увеличения «жесткости» (надежности) кабеля

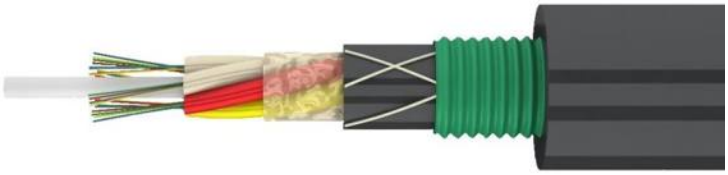
4. Дано:
Маскасети:255.255.255.248
АдресIP:192.168.1.219
Определите адрес сети.
а. 192.168.1.0
б. 192.168.1.255
в. 192.168.1.219
г. 192.168.1.218
д. 192.168.1.216
е. 192.168.1.223

5. Индикатор PoE на коммутаторе не горит, что обозначает:
а. устройство не исправно
б. устройство получает питание от источника переменного тока
или устройство не обнаружено.
в. коммутатор не исправен

6. Одной из первых задач при настройке коммутатора является
а. создание учетных записей пользователей
б. аутентификация пользователей
в. присвоение привилегий пользователям
7. MAC-адрес
а. это уникальный код, присвоенный производителем сетевому устройству, предполагается, что каждый код является уникальным для определённого устройства
б. это логические числовые адреса, назначаемые устройствам в компьютерной сети

8. Параметр Web Status на коммутаторе показывает
а. номер TCP-порта для Web-интерфейса
б. возможность настройки коммутатора через Web-интерфейс

9. На рисунке представлен



а. многопарный кабель типа «витая пара»
б. волоконно-оптический кабель

10. Изначально все порты коммутатора
а. не добавлены ни в одну VLAN
б. добавлены в одну VLAN с VID=1.

Ключи к тесту

Вариант 3		Вариант 4	
№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	б	1	б
2	а	2	б
3	б	3	б
4	б	4	д
5	а	5	б
6	а	6	а
7	вг	7	а
8	г	8	б
9	в	9	б
10	б	10	б

Шкала перевода баллов в отметки по пятибалльной системе

Оценка	Процент правильных ответов
5 (отлично)	от 70-100 %
4 (хорошо)	от 40-69,9 %
3 (удовлетворительно)	от 20-39,9%
2 (неудовлетворительно)	менее 19,9 %

3.2 Фонд оценочных средств для рубежного контроля по итогам первого семестра

Рубежный контроль проводится во время аудиторных занятий по профессиональному модулю

Вариант 1

1. Небольшая организация (5 сотрудников) собирается построить сеть. Какой тип сети является для нее наиболее приемлемым?
а. Одноранговая сеть
б. Сеть с выделенным сервером

2. Преимущества статической маршрутизации
а. Простота внедрения в небольшой сети
б. Высокий уровень безопасности
в. Все перечисленное

3. Коммутатор, поддерживающий оптические порты uplink, может быть подключен к SFP-портам с помощью
а. оптических кабелей
б. по витой паре неэкранированного/экранированного (UTP/STP) кабеля

4. Приведенный ниже пример иллюстрирует создание
а. учетной записи уровня пользователя
б. учетной записи уровня администратора

```
DES-3028:4# create account admin newmanager
Command: create account admin newmanager

Enter a case-sensitive new password: ********
Enter the new password again for confirmation: ********

Success.

DES-3028:4#
```

5. Посмотреть MAC-адрес коммутатора D-link можно с помощью ввода команды через интерфейс командной строки
а. show VLAN
б. show switch
в. show run

6. IP-адрес может быть установлен с помощью интерфейса командной строки CLI следующим образом:
а. config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy (где x –IP адрес, связанный с IP-интерфейсом (System); y – текущая маска подсети)
б. config ipif System ipaddress xxx.xxx.xxx.xxx/z (x – IP-адрес, связанный с IP-интерфейсом (System); z – соответствующее количество подсетей в CIDR нотации)
в. нет верного ответа

7. Поле State используется

а. для установления скорости и режимов работы (дуплекс/полудуплекс) для заданных портов
б. для включения и выключения заданных портов

8. В зависимости от конструктивного исполнения можно выделить следующие группы коммутаторов:
а. настольные коммутаторы, автономные коммутаторы, монтируемые в телекоммуникационную стойку, коммутаторы на основе шасси
б. управляемые, неуправляемые

9. Производительность коммутатора с 24 портами 10/100 Мбит/с и 2 портами 1 Гбит/с равна
а. 8,8 Гбит/с
б. 8,2 Гбит/с
в. 6,8 Гбит/с

10. Недостаточная емкость таблицы коммутации может стать причиной
а. замедления работы коммутатора
б. засорения сети избыточным широковещательным трафиком
в. все перечисленное

Вариант 2

1. Приведенный ниже пример иллюстрирует

```
DES-3028P:4#config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8

Success.

DES-3028P:4#_
```

а. создание учетной записи уровня администратора
б. назначение IP-адреса коммутатору

2. Заводской IP-адрес коммутатора D-Link по умолчанию
а. 10.90.90.90.
б. 10.10.10.90
в. 10.10.90.90

3. По возможности управления существуют категории коммутаторов:
а. неуправляемые, управляемые, настраиваемые коммутаторы
б. настольные, автономные, монтируемые в телекоммуникационную стойку

4. При работе в CLI есть возможность вводить сокращенный вариант команды
а. да
б. нет

5. Проверить созданную учетную запись на коммутаторе D Link можно с помощью команды
а. sh sw
б. show account
в. все перечисленное
г. нет верного ответа

6. Сброс настроек коммутатора D Link к заводским установкам выполняется с помощью команды
а. reboot
б. reset {[config I system]} {force_agree}

7. Возможность копировать переданные и принятые блоки данных на порт и перенаправлять копии на другой порт, к которому может быть подключено устройство, позволяющее осуществлять мониторинг трафика,
а. копирование портов
б. зеркалирование портов

8. На рисунке представлен результат выполнения команды

Port	State/ MDIX	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled Auto	10M/Full/Enabled	Link Down	Enabled
2	Enabled Auto	10M/Full/Enabled	Link Down	Enabled
3	Enabled Auto	10M/Full/Enabled	Link Down	Enabled

а. show ports 1-3
б. show account
в. save

9. На рисунке представлен результат выполнения команды

```
Device Type        : DES-3528 Fast Ethernet Switch
MAC Address        : 00-1E-58-50-15-10
IP Address         : 192.168.100.241 (Manual)
VLAN Name          : default
Subnet Mask        : 255.255.255.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 1.00.B007
Firmware Version   : Build 2.20.B028
Hardware Version   : A1
Serial Number      : P1UM186000004
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
VLAN Trunk         : Disabled
TELNET             : Enabled (TCP 23)
WEB                : Enabled (TCP 80)
SNMP               : Disabled
SSL Status         : Disabled
```

а. show account
б. show VLAN
в. show switch

10. Основными показателями коммутатора, характеризующими его производительность, являются:
а. скорость фильтрации кадров
б. скорость продвижения кадров
в. пропускная способность
г. задержка передачи кадра
д. все перечисленное

Ключи к тесту

Вариант 1		Вариант 2	
№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	а	1	б
2	в	2	а
3	а	3	а
4	б	4	а
5	б	5	б
6	аб	6	б
7	б	7	б

8	а	8	а
9	а	9	в
10	в	10	д

Шкала перевода баллов в отметки по пятибалльной системе

Оценка	Процент правильных ответов
5 (отлично)	от 70-100 %
4 (хорошо)	от 40-69,9 %
3 (удовлетворительно)	от 20-39,9%
2 (неудовлетворительно)	менее 19,9 %

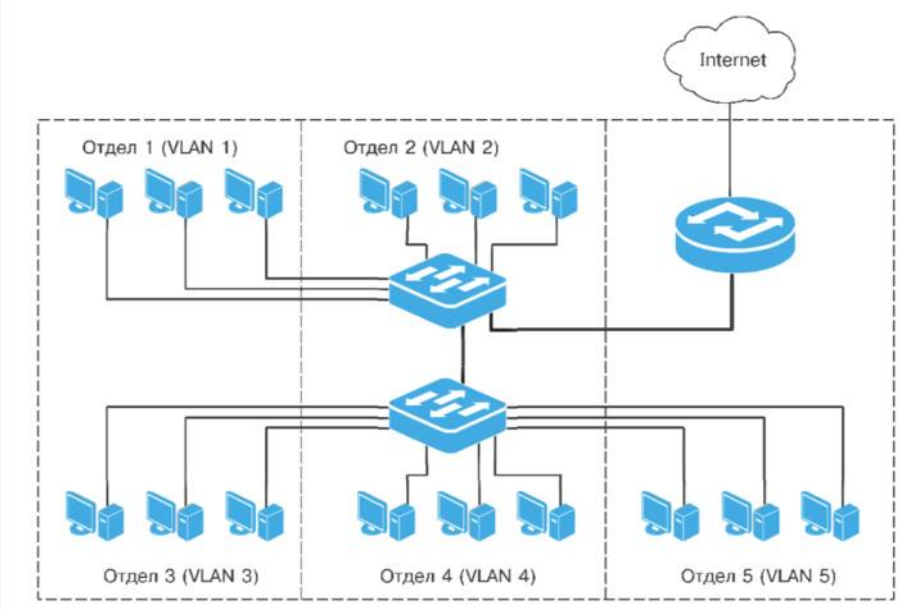
3.3 Фонд оценочных средств для промежуточной аттестации

На выполнение итоговой работы по модулю дается 18 академических часа, входящих в общее количество часов рабочей программы.

Вариант 1

1. Коммутатор Ethemet является устройством
а. канального уровня
б. сетевого уровня
г. физического уровня

2. На рисунке показана



а. физическая сегментация сети
б. логическая сегментация сети

3. Команда show fdb в коммутаторах D Link используется для
а. для отображения текущей таблицы коммутации
б. для отображения состояния внутреннего и внешнего питания коммутатора
в. для отображения статистики о переданных и полученных портом пакетах

4. WeЬ-интерфейс коммутатора
а. является альтернативой командной строке, обеспечивает графическое представление интерфейса управления коммутатором в режиме реального времени и предоставляет подробную информацию о состоянии портов, модулей, их типе и т.
б. не является альтернативой командной строке

5. Удалить учетную запись можно, выполнив команду
а. delete account <username>
б. delete< username>

6. Укажите проблемы, которые создают петли:
а. широковещательные штормы
б. множественные копии кадров
в. множественные петли
г. все перечисленное

7. Объединение нескольких физических портов в одну логическую магистраль на канальном уровне модели OSI с целью образования высокоскоростного канала передачи данных и повышения отказоустойчивости
а. агрегирование каналов связи
б. объединение широковещательных доменов

8. Отметьте характеристики, которые у портов, объединенных в агрегированный канал, должны быть настроены одинаково
а. тип среды передачи
б. скорость
в. режим работы
г. метод управления потоком
д. все перечисленные

9. Одновременная поддержка функций маршрутизации и коммутации, обязательная поддержка VLAN, реализация функций маршрутизации на аппаратном уровне с использованием ASIC характерна для
а. L3-коммутаторов
б. L2-коммутаторов

10. При физическом стекировании
а. комутаторы представляют собой разные логические устройства, но для уравления коммутаторами можно использовать интерфейс командной строки (CLI), WeЬ-интерфейс, Telnet, SSH, протокол SNMP, и только одному коммутатору (мастер-коммутатору) потребуется присвоение управляющего IP-адреса

б. коммутаторы представляют собой одно логическое устройство, для управления коммутаторами можно использовать интерфейс командной строки (CLI), WeЬ-интерфейс, Telnet, SSH, протокол SNMP, и только одному коммутатору (мастер-коммутатору) потребуется присвоение управляющего IP-адреса.

Вариант 2

1. Настройка даты и времени на коммутаторе D Link производится с помощью команды
а. show time
б. config time
в. show session

2. Активизаия функции шифрования паролей
а. enable password encryption
б. disable password encryption

3. Отключение воможности подключения к коммутатору по Telnet
а. enable telnet
б. disable telnet
в. не существует такой возможности

4. Просмотр статистики об ошибках передаваемых и принимаемых портом пакетов
а. show error ports 2
б. show utilization ports

5. Определение порта коммутатора, к которому подключено устройство с известным MAC-адресом
а. show fdb mac address
б. show fdb
в. нет правильного ответа

6. Функция Port Security
а. позволяет настроить какой-либо порт коммутатора так, чтобы через него доступ к сети мог осуществляться только определенными устройствами, устройства, которым разрешено подключаться к порту, определяются по MAC-адресам
б. позволяет настроить какой-либо порт коммутатора так, чтобы через него доступ к сети мог осуществляться только определенными устройствами, устройства, которым разрешено подключаться к порту, определяются по IP-адресам

7. Команда confiq port_security ports all admin_state enable max_learninq_ addr 1 позволяет
а. установить минимальное количество изучаемых каждым портом МАСадресов равным 1
б. установить максимальное количество изучаемых каждым портом МАСадресов равным 1

8. Для обеспечения QoS на канальном уровне модели OSI коммутаторы поддерживают стандарт IEEE 802.1p, который позволяет задать
а. до 8 уровней приоритетов (от 0 до 7, где 7 - наивысший)
б. до 8 уровней приоритетов (от 0 до 7, где 0 - наивысший)
в. до 15 уровней приоритетов (от 0 до 14, где 14 - наивысший)
г. до 15 уровней приоритетов (от 0 до 14, где 0 - наивысший)

9. SMTP (Simple Mail Transfer Protocol) – это
а. функция коммутатора, которая позволяет рассылать информацию о событиях, происходящих на коммутаторе, получателям электронной почты, адреса которых задаются с помощью указанных в данном разделе опций
б. функция коммутатора, которая позволяет сохранять информацию о событиях, происходящих на коммутаторе

10. Включение автоматической конфигурации адреса на интерфейсе
а. config ipif System ipv6 ipv6address fdd0:5f56 :d42c :134e : :1/64
б. config ipv6 nd ra ipif System state enable

Ключи к тесту

Вариант 1		Вариант 2	
№ вопроса	Верный ответ	№ вопроса	Верный ответ
1	а	1	б
2	б	2	а
3	а	3	б
4	а	4	а
5	а	5	а
6	г	6	а
7	а	7	а
8	д	8	а
9	а	9	а
10	б	10	б

4. Список литературы

1. Украинцев, Ю. Д., Основы телекоммуникаций : учебное пособие / Ю. Д. Украинцев. — Москва : КноРус, 2019. — 341 с. — ISBN 978-5-406-09678-9. — URL: https://book.ru/book/943635. — Текст: электронный.

2. Мельников, В. П., Информационная безопасность. : учебник / В. П. Мельников, А. И. Куприянов, ; под ред. В. П. Мельникова. — Москва : КноРус, 2019. — 267 с. — ISBN 978-5-406-10033-2. — URL: https://book.ru/book/944143. — Текст : электронный.

3. Ткаченко, С. Н., Методы и средства проектирования информационных систем и технологий + Приложение : учебник / С. Н. Ткаченко, Б. Р. Мищук. — Москва : КноРус, 2019. — 222 с. — ISBN 978-5-406-09467-9. — URL: https://book.ru/book/943815 — Текст : электронный.

Приложение 2

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 02. Организация сетевого администрирования

Специальность: 09.02.06 Сетевое и системное администрирование

2020

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ 02. Организация сетевого администрирования

1.1. Область применения программы профессионального модуля

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности: 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности: ПМ 02. Организация сетевого администрирования и соответствующих компетенций:

общие компетенции:

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	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.

профессиональные компетенции:

ПК 2.1	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2	Администрировать сетевые ресурсы в информационных системах.
ПК 2.3	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей
ПК 2.4	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля:

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

иметь практический опыт в:

– установке, настройке и сопровождении, контроле использования сервера и рабочих станций для безопасной передачи информации.

уметь:

– администрировать локальные вычислительные сети;

– принимать меры по устранению возможных сбоев;

– обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".

знать:

– основные направления администрирования компьютерных сетей;

– утилиты, функции, удаленное управление сервером;

– технологию безопасности, протоколов авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.

1.3. Количество часов на освоение программы профессионального модуля:

Общая нагрузка – **710 ч**., в том числе:
самостоятельная работа – **28 ч.**;
теоретические занятия– **102 ч.**;
практические занятия – **210 ч.**;
консультации – **10 ч.**;
учебная практика – **108 ч.;**
производственная практика – **180 ч;**
Курсовая работа – **30 ч.**
Квалификационный экзамен **– 18 ч.**

2.РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности Организация сетевого администрирования, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	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.

ПК 2.1	Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.
ПК 2.2	Администрировать сетевые ресурсы в информационных системах.
ПК 2.3	Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей
ПК 2.4	Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Общая	Учебная нагрузка							Практики	
			Самостоятельная работа	во взаимодействии с преподавателями							
				Всего по МДК	в том числе					Учебная	Производственная
					Теоретическое обучение	Лаб. Практ.	Курсов. работа	Консультации	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11	12
ОК 01- ОК 11 ПК 2.1 - 2.4	**Раздел1.** Сетевое и системное администрирование операционных систем	***211***	***15***	***196***	***42***	***106***	***30***	***6***	***12***		
ОК 01- ОК 11 ПК 2.1 - 2.4	**Раздел2.** Программное обеспечение компьютерных сетей	***98***	***10***	***88***	***32***	***48***		***2***	***6***		
ОК 01- ОК 11 ПК 2.1 - 2.4	**Раздел3.** Организация администрирования компьютерных сетей	***95***	***3***	***92***	***28***	***56***		***2***	***6***		
ОК 01- ОК 11 ПК 2.1 - 2.4	Учебная практика	***108***								***108***	
ОК 01- ОК 11 ПК 2.1 - 2.4	Производственная практика	***180***									***180***
	Квалификационный экзамен	***18***		***18***					***18***		
	Всего	***710***	***28***		***102***	***210***	***30***	***10***	***42***	***108***	***180***

3.2. Тематический план и содержание профессионального модуля ПМ 02. Организация сетевого администрирования инфраструктуры

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа	Объем часов	Коды компетенций
1		**2**	**3**	**4**
Раздел 1. МДК 02.01. Сетевое и системное администрирование операционных систем				
6 семестр				
Тема 1.	**Установка и настройка Windows Server 2012 R2**			
Тема 1.1. Развертывание и управление Windows Server 2012 R2		**Содержание учебного материала**		
	1	**Развертывание и управление Windows Server 2012 R2** Обзор Windows Server 2012R2. Установка Windows Server 2012R2. Настройка Windows Server 2012R2 после установки. Обзор задач по управлению Windows Server 2012R2. Введение в Windows PowerShell	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	2	ПЗ1.Обзор Windows Server 2012R2. Установка Windows Server 2012R2	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	3	ПЗ2.Обзор Windows Server 2012R2. Установка Windows Server 2012R2	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	4	ПЗ3.Введение в Windows PowerShell	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.2. Введение в доменные сервисы Службы Каталога		**Содержание учебного материала**		
	5	Введение в AD DS. Обзор функций контроллера домена. Установка контроллера домена	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
		Практические занятия		
	6	ПЗ4.Введение в AD DS. Обзор функций контроллера домена. Установка контроллера домена	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	7	ПЗ5.Установка контроллера домена	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.3. Управление объектами доменных служб Службы Каталога		**Содержание учебного материала**		
	8	Управление учетными записями пользователей. Управление группами. Управление учетными записями компьютеров. Делегирование административных задач	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	9	ПЗ6. Управление учетными записями пользователей. Управление группами. Управление учетными записями компьютеров. Делегирование административных задач	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.4. Автоматизация администрирования доменных служб Службы Каталога		**Содержание учебного материала**		
	10	Использование средств командной строки для администрирования AD DS**.** Использование Windows PowerShell для администрирования AD DS. Произведение множественных операций с использованием Windows PowerShell.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	11	ПЗ7.Использование средств командной строки для администрирования AD DS**.** Использование Windows PowerShell для администрирования AD DS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	12	ПЗ8.Установка роли DHCP сервер**.** Настройка DHCP областей**.** Управление базой данных DHCP**.** Защита и мониторинг DHCP	*2*	ОК 01-ОК 11

				ПК 2.1 - 2.4
	13	ПЗ.9Настройка DHCP областей**.** Управление базой данных DHCP**.** Защита и мониторинг DHCP	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	14	ПЗ10.Процесс разрешения имен в Windows. Установка сервера DNS. Управление зонами DNS	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.5. Применение локального хранилища данных		**Содержание учебного материала**		
	15	Обзор методов хранения данных. Управление дисками и томами. Использование пространств хранения	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	16	ПЗ11. Управление дисками и томами. Использование пространств хранения	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.6. Применение файловой службы и службы печати		**Содержание учебного материала**		
	17	Защита файлов и папок. Защита папок средствами теневого копирования. Настройка Рабочих папок. Настройка сетевой печати	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	18	ПЗ12.Защита файлов и папок. Настройка Рабочих папок. Настройка сетевой печати	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.7.		**Содержание учебного материала**		

Применение групповой политики	19	Обзор групповой политики. Обработка групповых политик. Применение централизованного хранилища Административных шаблонов	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	20	ПЗ13.Обзор групповой политики. Обработка групповых политик	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	21	ПЗ14.Применение централизованного хранилища Административных шаблонов	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.8. Защита серверов Windows применением объектов групповой политики		**Содержание учебного материала**		
	22	Обзор безопасности операционных систем Windows**.** Настройка параметров безопасности. Ограничение прикладного ПО. Настройка брандмауэра Windows с расширенной безопасностью	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	23	ПЗ15.Ограничение прикладного ПО. Настройка брандмауэра Windows с расширенной безопасностью	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	24	ПЗ.16 ПрименениеHyper-V. Управление хранилищем виртуальных машин. Управление виртуальными сетями	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.		**Администрирование Windows Server 2012 R2**		
Тема 2.1. Настройка и устранение неполадок службы DNS		**Содержание учебного материала**		
	25	Настройка серверной роли DNS. Настройка зон DNS. Настройка передачи зоны DNS. Управление службой DNS и устранение неполадок	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
		Практические занятия		
	26	ПЗ17.Настройка серверной роли DNS. Настройка зон DNS. Настройка передачи зоны DNS. Управление службой DNS и устранение неполадок	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	27	ПЗ18.Настройка и устранение неполадок службы DNS		
		Лабораторные работы не предусмотрены		
Тема 2.2. Поддержка доменных служб Службы Каталога		**Содержание учебного материала**		
	28	Обзор AD DS. Использование виртуализированных контроллеров домена. Применение контроллеров домена с доступом только на чтение (RODC). Администрирование AD DS. Управление базой данных AD DS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	29	ПЗ19. Применение контроллеров домена с доступом только на чтение (RODC). Администрирование AD DS. Управление базой данных AD DS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	30	ПЗ20.Поддержка ADDS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	31	ПЗ21.Настройка Политики паролей и Политики блокировки учетной записи. Настройка Управляемой служебной учетной записи	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	32	ПЗ22.Управление пользовательскими и служебными учетными записями	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.3. Внедрение инфраструктуры Групповых политик		**Содержание учебного материала**		
	33	Обзор Групповой политики. Внедрение и администрирование Групповых политик. Область действия и порядок обработки Групповых политик. Устранение неполадок	*2*	ОК 01-ОК 11

		применения Групповых политик		ПК 2.1 - 2.4
		Практические занятия		
	34	ПЗ23Область действия и порядок обработки Групповых политик. Устранение неполадок применения Групповых политик	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.4. Управление пользовательским рабочим столом через Групповую политику		**Содержание учебного материала**		
	35	Применение Административных шаблонов. Настройка применения скриптов и перенаправления папок. Настройка предпочтений в Групповой политике. Управление программным обеспечением через Групповую политику	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	36	ПЗ24Настройка предпочтений в Групповой политике. Управление программным обеспечением через Групповую политику	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	37	ПЗ25.Внедрение инфраструктуры Групповых политик	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	38	ПЗ26.Управление пользовательским рабочим столом через Групповую политику	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	39	ПЗ27.Установка и настройка роли Сервер Сетевой политики. Настройка клиентов и серверов RADIUS. Методы проверки подлинности сервера Сетевой политики. Мониторинг и устранение неполадок роли Сервер Сетевой политики	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	40	ПЗ28.Установка и настройка роли Сервер Сетевой политики	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4

	41	ПЗ.29. Настройка NAP. Настройка применения NAP через принудительные IPSec взаимодействия. Мониторинг и устранение неполадок NAP	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	42	ПЗ.30Применение защиты доступа к сети	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.5. Использование удаленного доступа		**Содержание учебного материала**		
	43	Обзор технологии удаленного доступа. Внедрение технологии DirectAccess с помощью мастера начальной настройки. Внедрение и управление расширенной инфраструктурой DirectAccess. Внедрение VPN. Внедрение Web Application Proxy	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	44	ПЗ31.Внедрение и управление расширенной инфраструктурой DirectAccess. Внедрение VPN. Внедрение Web Application Proxy	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	45	ПЗ32.Внедрение технологии DirectAccess с помощью мастера начальной настройки	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	46	ПЗ33.Развертывание расширенной инфраструктуры DirectAccess	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	47	ПЗ34.Внедрение VPN	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	48	ПЗ35.Внедрение Web Application Proxy	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
		Лабораторные работы не предусмотрены		
Тема 2.6. Оптимизация файловых сервисов		**Содержание учебного материала**		
	49	Обзор диспетчера ресурсов файлового сервера – FSRM. Использование FSRM для управления квотами, файловым экранированием и отчетами по использованию хранилища. Применение классификации файлов и задач по управлению файлами. Обзор распределенной файловой системы DFS. Настройка именованного пространства DFS. Настройка и устранение неполадок репликации DFS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	50	ПЗ36.Настройка именованного пространства DFS. Настройка и устранение неполадок репликации DFS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Консультация	51	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Экзамен	***6***	
		Всего: 180/72 (0)		
		7 семестр		
		Практические занятия		
	52	ПЗ37.Настройка Квот и файлового экранирования в FSRM	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	53	ПЗ38.Применение DFS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	54	ПЗ39.Шифрование дисков с использованием BitLocker. Шифрование файлов с использованием EFS. Настройка расширенного аудита.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

	55	ПЗ40.Настройка шифрования и расширенного аудита	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.7. Развертывание и поддержка серверных образов		**Содержание учебного материала**		
	56	Обзор службы развертывания Windows. Управление образами. Применение развертывания с помощью службы развертывания Windows. Администрирование службы развертывания Windows.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	57	ПЗ41.Администрирование службы развертывания Windows.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.8. Внедрение управления обновлениями		**Содержание учебного материала**		
	58	Обзор WSUS. Развертывание обновлений посредством WSUS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	59	ПЗ42.Использование службы развертывания Windows для развертывания WindowsServer 2012	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	60	ПЗ43.Внедрение управления обновлениями	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	61	ПЗ44.Средства мониторинга. Использование Монитора производительности. Мониторинг журналов событий.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

	62	ПЗ45.Мониторинг WindowsServer 2012	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 3.		**Основы Linux**		
Тема 3.1. VMWare vSphere		**Содержание учебного материала**		
	63	Введение в дисциплину. Знакомство с VMWare vSphere.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	64	ПЗ46.Введение в дисциплину. Знакомство с VMWare vSphere.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 3.2. Файловые системы ОС Linux		**Содержание учебного материала**		
	65	Файловые системы ОС Linux. Создание и разметка жесткого диска	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	66	ПЗ47.Файловые системы ОС Linux. Создание и разметка жесткого диска	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	67	ПЗ48. Подготовка сервера ОС Linux. Разметка жесткого диска.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	68	ПЗ49. Настройка web-серверов в ОС Linux. Протокол HTTP. Веб-сервер Nginx. Обратное проксирование в Nginx.	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
	69	ПЗ50. Протокол DNS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	70	ПЗ51.Настройка сервера DHCP в ОС Linux. Протокол DHCP	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 3.3. Настройка файловых серверов в ОС Linux		**Содержание учебного материала**		
	71	**Настройка файловых серверов в ОС Linux** Протокол FTP. Файловая система NFS. Файловый сервер Samba.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	72	ПЗ52.Протокол FTP. Файловая система NFS. Файловый сервер Samba.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 3.4. Настройка серверов БД в ОС Linux		**Содержание учебного материала**		
	73	**Настройка серверов БД в ОС Linux** СУБД MySQL. СУБД MongoDB	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	74	ПЗ№53Контейнеры Docker.Способы связи контейнеров Docker.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 3.5. Проектирование		**Содержание учебного материала**		
	75	Проектирование. Введение. Анализ требований. Реализация системы. Составление	*2*	ОК 01-

		документации		ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	76	Выбор темы курсовой работы	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	77	Подбор, изучение, анализ литературы по выбранной теме	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	78	Отбор фактического материала по выбранной теме	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	79	Отбор фактического материала по выбранной теме	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	80	Требования к структуре курсовой работы	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	81	Требования к содержанию курсовой работы	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		

	82	Составление плана курсовой работы	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	83	Написание введения и заключения курсовой работы	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	84	Стиль изложения научных материалов	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	85	Технические требования к оформлению	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	86	Технические требования к оформлению	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	87	Рецензирование курсовых работ	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	88	Подготовка речи к выступлению	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

Курсовая работа		**Содержание материала**		
	89	Защита курсовой работы	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Курсовая работа		**Содержание материала**		
	90	Защита курсовой работы	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Самостоятельная работа		
	91	Администрирование службы развертывания Windows.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	92	Мониторинг журналов событий.	*2*	
	93	Настройка Квот и файлового экранирования в FSRM	*2*	
	94	Настройка именованного пространства DFS.	*2*	
	95	Настройка и устранение неполадок репликации DFS	*2*	
	96	Развертывание расширенной инфраструктуры DirectAccess	*2*	
	97	Применение защиты доступа к сети	*2*	
	98	Групповые политики	*1*	
Консультация	99	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Консультация	100	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Экзамен	***6***	
		Всего: 103/34(15)		
		Всего: 211/106(15)		

6 семестр

Наименование разделов и тем профессионального	**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа**	**Объем часов**	**Коды компетен**

модуля (ПМ), междисциплинарных курсов (МДК)				**ций**
1	**2**		**3**	**4**
Раздел 2. МДК.02.02	**Программное обеспечение компьютерных сетей**			
Тема 1.	**Маршрутизация и коммутация. Масштабирование сетей.**			
Тема 1.1. Реализация клиентской инфраструктуры		**Содержание учебного материала**		
	1	Оценка и определение параметров развертывания клиентских ОС Обзор жизненного цикла клиентских компьютеров предприятия. Оценка оборудования и готовности инфраструктуры к развертыванию клиентских ОС. Обзор методов развертывания клиентских ОС в среде организации. Технологии лицензионной активации для клиентских компьютеров в организации. Планирование стратегии развертывания клиентских ОС. Сбор данных об инфраструктуре. Реализация решения лицензионной активации. Планирование стратегии управления образами Обзор форматов образа Windows. Обзор средств управления образами (Image Management). Оценка бизнес-требований для поддержки стратегии управления образами.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.2. Реализация безопасности клиентских систем	2	Реализация централизованного решения по безопасности клиентских ОС. Планирование и реализация BitLocker. Планирование и реализация шифрования с помощью EFS. Настройка безопасности клиентских ОС с помощью групповой политики. Настройка шифрования диска с помощью BitLocker. Реализация решения централизованного управления EFS. Реализация решения для восстановления файлов, защищенных EFS.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.3. Захват и управление образами клиентских ОС	3	Захват и управление образами клиентских ОС Обзор Windows ADK. Управление средой предустановки Windows (Windows PE). Создание исходного образа с помощью Windows SIM и Sysprep. Захват и обслуживанию эталонного образа. Настройка и управление службой развертывания Windows (Windows Deployment Services). Настройка Windows PE. Установка эталонного компьютера с помощью файла ответов. Обработка эталонного компьютера с помощью Sysprep. Создание файла ответов с помощью Windows SIM. Установка эталонного компьютера с помощью файла ответов. Обработка эталонного компьютера с помощью Sysprep. Services Планирование среды WindowsDeploymentServices. Установка и настройка серверной роли WDS. Захват эталонного образа с помощью WDS. Развертывание образа с помощью WDS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

Тема 1.4. Планирование и реализация миграции пользовательской среды	4	Планирование и реализация миграции пользовательской среды Обзор способов миграции пользовательской среды. Планирование миграции пользовательской среды с помощью USMT. Миграция состояния пользователя с помощью USMT. Планирование миграции пользовательской среды. Создание и настройка XML-файлов USMT. Сбор данных и восстановления профиля пользователя с помощью USMT. Выполнение миграции с созданием жестких ссылок	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.5. Планирование и развертывание клиентских ОС с помощью Microsoft Deployment Toolkit	5	Планирование и развертывание клиентских ОС с помощью Microsoft Deployment Toolkit Планирование среды Lite Touch Installation. Реализация MDT 2012 для Lite Touch Installation. Интеграция служб развертывания Windows с MDT. Планирование среды Lite Touch Installation. Установка MDT 2012 и необходимых компонентов. Создание и настройка MDT 2012 Deployment Share. Развертывание и захват образа эталонной ОС. Интеграция WDS с MDT 2012 для обеспечения возможностей загрузки PXE.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.6. Планирование и развертывание клиентских ОС с помощью System Center Configuration Manager 2012	6	Планирование и развертывание клиентских ОС с помощью System Center Configuration Manager 2012 Планированиесреды Zero Touch Installation. Подготовка сайта для развертывания ОС. Построение эталонного образа на основе последовательности задач Configuration Manager. Использование последовательности задач MDT для развертывания клиентских образов. Планирование инфраструктуры развертывания операционной системы. Подготовка среды Zero Touch Installation. Настройка пакетов развертывания и образов системы. Подготовка среды ZeroTouchInstallation	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.7. Планирование и реализация служб удаленного доступа (Remote Desktop Services)	7	Планирование и реализация служб удаленного доступа (Remote Desktop Services) Обзор службы удаленного рабочего стола. Планирование среды Remote Desktop Services. Настройка развертывания инфраструктуры виртуальных рабочих столов. Настройка доступа к клиентам на основе сеансов (Session-Based Desktop). Расширение среды Remote Desktop Services в Интернет. Планирование среды Remote Desktop Services. Настройка сценария инфраструктуры виртуальных рабочих столов. Настройка сценария доступа на основе сеансов. Проектирование политик шлюзов RDS. Настройка шлюзов RDS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.8. Управление виртуализацией пользовательского состояния для клиентских ОС организации	8	Управление виртуализацией пользовательского состояния для клиентских ОС организации Обзор виртуализации профиля пользователя. Планирование виртуализации профиля пользователя. Настройка перемещаемых профилей, перенаправления папок и автономных (offline) файлов. Реализация виртуализации работы пользователя от	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

		Microsoft (Microsoft User Experience Virtualization). Планирование виртуализации профиля пользователя. Реализация виртуализации профиля пользователя.		
		Практические занятия		
	9	ПЗ1.Оценка и определение параметров развертывания	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	10	ПЗ2.Планирование стратегии управления образами	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	11	ПЗ3.Настройка безопасности клиентских систем	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	12	ПЗ4.Настройка шифрования файлов с помощью EFS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	13	ПЗ5.Подготовка образа и среды предустановки Установка Windows ADK	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	14	ПЗ6.Создание эталонного образа с помощью Windows SIM и Sysprep Создание файла ответов с помощью Windows SIM	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	15	ПЗ7.Создание и обслуживание эталонного образа	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	16	ПЗ8.Настройка и управление Windows Deployment Services Планирование среды Windows Deployment Services	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
	17	ПЗ9.Планирование и реализация миграции пользовательской среды	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.9. Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организации		**Содержание учебного материала**		
	18	Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организации Планирование инфраструктуры обновлений для организации. Реализация поддержки обновлений программного обеспечения с помощью Configuration Manager 2012. Управление обновлениями для виртуальных машин и образов. Использование Windows Intune для управления обновление программного обеспечения. Планирование инфраструктуры обновления. Реализация обновлений программного обеспечения с помощью Configuration Manager 2012. Реализация обновлений программного обеспечения для библиотек виртуальных машин.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.10. Защита компьютеров предприятия от вредоносных программ и потерь данных	19	Защита компьютеров предприятия от вредоносных программ и потерь данных Обзор System Center 2012 Endpoint Protection. Настройка Endpoint Protection Client Settings и мониторинга состояния. Использование Windows Intune Endpoint Protection. Защита клиентских ОС с помощью System Center 2012 Data Protection Manager. Настройка и развертывание политик EndpointProtection. Настройка параметров клиента для поддержки Endpoint Protection. Мониторинг защиты конечных точек. Настройка и проверка защиты данных клиента	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.11. Мониторинг производительности и работоспособности инфраструктуры клиентских ОС	20	Мониторинг производительности и работоспособности инфраструктуры клиентских ОС. Производительность и работоспособность инфраструктуры клиентских ОС. Мониторинг инфраструктуры виртуальных клиентов. Настройка Operations Manager для мониторинга виртуальных сред.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	21	ПЗ10.Миграция состояния пользователя с созданием жестких ссылок	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

	22	ПЗ11.Планирование и развертывание клиентских ОС с помощью MDT	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	23	ПЗ12.Подготовка среды для развертывания операционной системы	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	24	ПЗ13.Использование MDT и Configuration Manager для подготовки Zero-Touch Installation	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	25	ПЗ14.Планирование и реализация инфраструктуры Remote Desktop Services	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	26	ПЗ15.Расширение доступа к Интернет для инфраструктуры RDS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	27	ПЗ16.Развертывание и поддержка виртуализации профиля пользователя	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	28	ПЗ17.Проектирование и реализация файловых служб	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	29	ПЗ18.Реализация Client Endpoint Protection Настройка точки Endpoint Protection	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	30	ПЗ19.Настройка Data Protection для данных клиентского компьютера	*2*	ОК 01-ОК 11

				ПК 2.1 - 2.4
	31	ПЗ20.Мониторинг производительности и работоспособности инфраструктуры клиентских ОС Настройка	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Тема 2.		**Реализация среды настольных приложений.**		
Тема 2.1. Разработка стратегии развертывания приложений		**Содержание учебного материала**		
	32	Определение бизнес-требований для развертывания приложений. Обзор стратегии развертывания приложений. Выбор подходящей стратегии развертывания приложений для офиса.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	33	ПЗ21.**Диагностика и обеспечение совместимости приложений** Диагностика проблем совместимости приложений. Оценка и реализация решений по восстановлению. Решение проблемы совместимости с помощью Application Compatibility Toolkit. Установка и настройка ACT. Анализ потенциальных проблем совместимости. Решение проблем совместимости приложений. Автоматизация развертывания программных средств обеспечения совместимости (shims)	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
	34	ПЗ22.**Развертывание приложений с помощью групповых политик и Windows Intune** Развертывание приложений с помощью групповых политик. Развертывание приложений с помощью Windows Intune. Развертывание приложений с помощью групповых политик. Запуск симуляции Windows Intune.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.1. Развертывание приложений с помощью System Center Configuration Manager		**Содержание учебного материала**		
	35	Развертывание приложений с помощью System Center Configuration Manager Концепции развертывания приложений с помощью Configuration Manager 2012. Развертывание приложений с помощью Configuration Manager 2012. Создание запросов Configuration Manager 2012. Создание коллекций пользователей и устройств Configuration Manager 2012.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	36	ПЗ23.**Развертывания самообслуживаемых приложений** Концепции развертывания самообслуживаемых приложений. Настройка	*2*	ОК 01- ОК 11

		самообслуживаемых приложений с Windows Intune. Развертывания самообслуживаемых приложений с Configuration Manager 2012. Развертывания самообслуживаемых приложений с Service Manager 2012. Подготовка System Center Configuration Manager 2012 для поддержки Service Manager 2012 Self-Service Portal. Настройка ServiceManager 2012 Self-ServicePortal. Проверка возможности предоставления приложений пользователям с помощью Self-Service Portal.		ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.2. Проектирование и реализация инфраструктуры виртуализации представлений		**Содержание учебного материала**		
	37	Проектирование и реализация инфраструктуры виртуализации представлений Оценка требований виртуализации представлений. Планирование инфраструктуры виртуализации представлений. Развертывание инфраструктуры виртуализации представлений. Развертывание инфраструктуры высокой готовности для виртуализации представлений .Подготовка, настройка и развертывание представлений виртуализации приложений. Определение стратегии представлений виртуализации приложений. Развертывание удаленного рабочего стола, RemoteApp, и RD Web Access. Развертывание приложений на RD Session Host. Настройка и развертывание приложений RemoteApp. Проверка возможности использования приложений с помощью RD Web Access.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
Тема 2.3. Проектирование и развертывание среды виртуализации приложений		**Содержание учебного материала**		
	38	Проектирование и развертывание среды виртуализации приложений Обзор моделей виртуализации приложений. Развертывание компонентов инфраструктуры виртуализации приложений. Настройка клиентской поддержки виртуализации приложений. Планирование развертывания App-V ролей и компонентов. Развертывание инфраструктуры App-V. Настройка клиента App-V. Подготовка приложений для выполнения в среде App-V. Развертывание приложений App-V.. Подготовка приложений к виртуализации. Развертывание App-V приложений с помощью Configuration Manager.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	39	П324.**Планирование и реализация безопасности и обновления приложений** Планирование обновления приложений. Развертывание обновлений с помощью WSUS. Развертывание обновлений с помощью Configuration Manager 2012. Реализация безопасности приложений. Обновление развернутых приложений. Обновление приложений App-V. Развертывание политик AppLocker для управления запуском приложений.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4

		Лабораторные работы не предусмотрены		
Тема 2.4. Планирование и реализация обновления и замены приложений		**Содержание учебного материала**		
	40	Планирование и реализация обновления и замены приложений Планирование и реализация обновления приложений и замещения приложений.. Обновление развернутых приложений. Замена развернутых приложений. Настройка сосуществования. Мониторинг развертывания, использования и производительности приложений. Планирование и реализация инфраструктуры мониторинга приложений. Метрики, инвентаризация и анализ ресурсоемкости приложений. Мониторинг использования ресурсов приложений. Планирование инвентаризации приложений. Организация инвентаризации программного обеспечения. Метрики использования приложений. Мониторинг использование ресурсов серверов RD Session Host приложениями.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Самостоятельная работа		
	41	Выбор подходящей стратегии развертывания приложений для офиса.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	42	Проектирование и реализация инфраструктуры виртуализации представлений	*2*	
	43	Планирование и реализация сосуществования приложений	*2*	
	44	Установка и настройка App-V Sequencer	*2*	
	45	Снижение пиковой нагрузки на ресурсы приложениями различных версий приложения	*2*	
Консультация	46	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Экзамен	***6***	
		Всего: 98/48(10)		

7 семестр				
Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)		**Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа**	**Объем часов**	**Коды компетенций**
	1	**2**	**3**	**4**
Раздел 3.		**Организация администрирования компьютерных систем**		
МДК.02.03.		**Организация администрирования компьютерных систем**		
Тема 1.		**Организация администрирования компьютерных систем**		

Тема 1.1 Планирование апгрейда и миграции сервера		**Содержание учебного материала**		
	1	Планирование апгрейда и миграции сервера Рекомендации по апгрейду и миграции. Создание плана апгрейда и миграции сервера. Планирование виртуализации	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	2	ПЗ1. Создание плана апгрейда и миграции сервера. Планирование виртуализации	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.2 Планирование и внедрение инфраструктуры для развертывания серверов		**Содержание учебного материала**		
	3	Планирование и внедрение инфраструктуры для развертывания серверов Выбор подходящей стратегии создания образов сервера. Внедрение стратегии автоматического развертывания	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	4	ПЗ2. Планирование и развертывание серверов с использованием диспетчера виртуальных машин (VMM) Обзор диспетчера виртуальных машин в System Center 2012 R2. Реализация библиотек и профилей диспетчера виртуальных машин.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	5	ПЗ3.Планирование и развертывание служб VMM.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	6	ПЗ4.Реализация библиотек и профилей диспетчера виртуальных машин. Планирование и развертывание служб VMM.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	7	ПЗ5. Проектирование и внедрение инфраструктуры лесов и доменов Active Directory Domain Services Проектирование леса AD DS. Проектирование и реализация доверительных отношений между лесами. Проектирование интеграции ADDS с WindowsAzureActiveDirectory.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4

	8	ПЗ6. Проектирование и создание доменов AD DS. Проектирование пространств имен DNS в среде AD DS. Проектирование доверительных отношений AD DS.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.3 Проектирование и реализация инфраструктуры подразделений (OU) и разрешений AD DS		**Содержание учебного материала**		
	9	Проектирование и реализация инфраструктуры подразделений (OU) и разрешений AD DS. Планирование делегирования административных задач. Проектирование структуры подразделений OU. Проектирование и внедрение стратегии групп AD DS	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 1.4 Проектирование и внедрение стратегии групповых политик		**Содержание учебного материала**		
	10	Проектирование и внедрение стратегии групповых политик Сбор требуемой информации для проектирования групповых политик. Проектирование и внедрение групповых политик. Проектирование обработки групповых политик. Планирование управления групповыми политиками	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	11	ПЗ7.Проектирование и внедрение групповых политик. Проектирование обработки групповых политик. Планирование управления групповыми политиками	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	12	ПЗ8.Проектирование и реализация физической топологии AD DS Проектирование и реализация сайтов Active Directory. Проектирование репликации Active Directory.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	13	ПЗ9.Проектирование размещения контроллеров домена. Виртуализация контроллеров домена. Проектирование высокой доступности контроллеров домена	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.5 Планирование и реализация хранилищ данных		**Содержание учебного материала**		
	14	Планирование и реализация хранилищ данных Планирование и внедрение iSCSI SAN. Планирование и внедрение Storage Spaces. Оптимизация файловых служб для филиалов.	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
		Практические занятия		
	15	ПЗ10.Планирование и внедрение iSCSI SAN. Планирование и внедрение Storage Spaces. Оптимизация файловых служб для филиалов.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 1.6 Планирование и реализация защиты сетей		**Содержание учебного материала**		
	16	Планирование и реализация защиты сетей Обзор проектирования безопасности сетей. Проектирование и внедрение использования Windows Firewall. Проектирование и внедрение инфраструктуры NAP	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	17	ПЗ11.Проектирование и реализация защиты служб доступа к сети Планирование и внедрение DirectAccess. Планирование и внедрение VPN.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	18	ПЗ12.Планирование и внедрение Web Application Proxy. Планирование сложной инфраструктуры удаленного доступа	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.		**Реализация продвинутой серверной инфраструктуры**		
Тема 2.1 Обзор управления Центром Обработки Данных предприятия		**Содержание учебного материала**		
	19	Обзор управления Центром Обработки Данных предприятия Обзор ЦОД предприятия. Обзор компонент SystemCenter 2012 R2	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 2.2 Планирование и реализация стратегии виртуализации серверов		**Содержание учебного материала**		
	20	Планирование и реализация стратегии виртуализации серверов Планирование развертывания диспетчера виртуальных машин (VMM). Планирование и реализация серверной виртуализации.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 2.3		**Содержание учебного материала**		

Планирование и реализация сетевой инфраструктуры и систем хранения данных для виртуализации	21	Планирование и реализация сетевой инфраструктуры и систем хранения данных для виртуализации Планирование систем хранения для виртуализации. Реализация систем хранения для виртуализации. Планирование и реализация сетевой инфраструктуры для виртуализации. Планирование и реализация виртуализации сети	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	22	ПЗ13.Планирование и реализация сетевой инфраструктуры для виртуализации. Планирование и реализация виртуализации сети	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.4 Планирование и развертывание виртуальных машин		**Содержание учебного материала**		
	23	Планирование и развертывание виртуальных машин Планирование параметров виртуальных машин. Подготовка к развертыванию виртуальных машин с использованием диспетчера виртуальных машин (VMM). Развертывание виртуальных машин. Планирование и реализация реплики Hyper-V	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 2.5 Планирование и реализация решения по администрированию виртуализации		**Содержание учебного материала**		
	24	Планирование и реализация решения по администрированию виртуализации Планирование и реализация автоматизации с использованием System Center 2012 R2. Планирование и реализация MicrosoftSystemCenterAdministration. Планирование и реализация Self-Service с использованием System Center 2012 R2. Планирование и реализация установки обновлений в инфраструктуре серверной виртуализации	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	25	ПЗ14.Планирование и реализация Self-Service с использованием System Center 2012 R2. Планирование и реализация установки обновлений в инфраструктуре серверной виртуализации	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	26	ПЗ15.Планирование и реализация Self-Service с использованием System Center 2012 R2. Планирование и реализация установки обновлений в инфраструктуре серверной виртуализации	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	27	ПЗ16.Планирование и реализация стратегии мониторинга серверов. Планирование мониторинга в Windows Server 2012 R2. Обзор SystemCenterOperationsManager.	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
	28	ПЗ17Планирование и настройка компонент мониторинга. Настройка взаимодействия с VMM Планирование и настройка компонент мониторинга. Настройка взаимодействия с VMM	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	29	ПЗ18. Планирование и реализация решений высокой доступности для файловых служб и приложений.Планирование и реализация Storage Spaces. Планирование и реализация DFS. Планирование и реализация NLB	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Лабораторные работы не предусмотрены		
Тема 2.6 Планирование и реализация решений высокой доступности на основе кластеров		**Содержание учебного материала**		
	30	Планирование и реализация решений высокой доступности на основе кластеров Планирование инфраструктуры отказоустойчивых кластеров. Внедрение отказоустойчивого кластера. Планирование и реализация системы установки обновлений для отказоустойчивого кластера. Интеграция отказоустойчивых кластеров и виртуализации. Планирование распределённых отказоустойчивых кластеров	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
Тема 2.7 Планирование и реализация стратегии бесперебойной работы (Business Continuity Strategy)		**Содержание учебного материала**		
	31	Планирование и реализация стратегии бесперебойной работы (Business Continuity Strategy) Обзор стратегии бесперебойной работы. Планирование и реализация стратегий резервного копирования. Планирование и реализация восстановления. Планирование и реализация резервного копирования и восстановления виртуальных машин	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Практические занятия		
	32	ПЗ19. Планирование и реализация инфраструктуры открытых ключей Планирование и развертывание удостоверяющих центров. Планирование и реализация шаблонов сертификатов. Планирование и реализация выдачи и отзыва сертификатов. Планирование и реализация архивации и восстановления ключей	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	33	ПЗ20.Планирование и развертывание AD FS Планирование и реализация инфраструктуры AD FS. Планирование и реализация AD FS Claim Providers и Relying Parties. Планирование и реализация AD FS Claims и Claim Rules. Планирование и реализация Web Application Proxy	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	34	ПЗ21.Планирование и реализация доступа к данным для пользователей и устройств Планирование и реализация DAC. Планирование подключения к рабочему месту (Workplace Join). Планирование рабочих папок (Work Folders)	*2*	ОК 01-ОК 11 ПК 2.1 -

				2.4
	35	ПЗ22.Планирование и реализация службы управления правами Обзор AD RMS. Планирование и реализация кластера AD RMS. Планирование и внедрение шаблонов AD RMS и политик AD RMS. Планирование и реализация внешнего доступа к AD RMS. Планирование и реализация взаимодействия AD RMS и Dynamic Access Control.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	36	ПЗ23.Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	37	ПЗ24.Установка прав доступа и контроль использования сетевых ресурсов	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	38	ПЗ25.Администрирование серверов	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	39	ПЗ26.Расчёт стоимости сетевого оборудования и программного обеспечения	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	40	ПЗ27.Регистрация пользователей локальной сети	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	41	ПЗ28.Осуществление антивирусной защиты	*2*	ОК 01-ОК 11 ПК 2.1 - 2.4
	42	**Лабораторные работы не предусмотрены**		
		Самостоятельная работа		
	43	Расчёт стоимости сетевого оборудования	*2*	ОК 01-ОК 11

				ПК 2.1 - 2.4
	44	Расчёт стоимости программного обеспечения	*1*	ОК 01- ОК 11 ПК 2.1 - 2.4
Консультация	45	Повторение и обобщение изученного материала. Подготовка к экзамену.	*2*	ОК 01- ОК 11 ПК 2.1 - 2.4
		Экзамен	*6*	
		Всего: 95/56(3)		
Учебная практика		**Виды работ**	***108***	
	1	Администрирование серверов и рабочих станций.	*18*	ОК 01- ОК 11 ПК 2.1 - 2.4
	2	Организация доступа к локальным сетям и Интернету.	*18*	
	3	Установка и сопровождение сетевых сервисов.	*18*	
	4	Расчёт стоимости сетевого оборудования и программного обеспечения.	*18*	
	5	Сбор данных для анализа использования программно-технических средств компьютерных сетей.	*18*	
	6	Обеспечение сетевой безопасности	*18*	
Производственная практика		**Виды работ**	***180***	
	1	Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.	*36*	ОК 01- ОК 11 ПК 2.1 - 2.4
	2	Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.	*18*	
	3	Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.	*18*	
	4	Обеспечение своевременного копирования, архивирования и резервирования данных.	*18*	
	5	Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования. Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.	*18*	
	6	Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.	*18*	
	7	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к	*36*	

		информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.		
	8	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	*36*	ОК 01-ОК 11 ПК 2.1 - 2.4
		Квалификационный экзамен	***18***	
		Всего:	***710/210(28)***	

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля требует наличия следующих специальных помещений:

Лаборатория «Организация и принципы построения компьютерных систем», оснащенная в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

Для выполнения практических лабораторных занятий курса в группах (до 15 человек) требуются компьютеры и периферийное оборудование в приведенной ниже конфигурации:

– 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, лицензионный 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, FRC 2068 — HTTP,

RFC 2131 — DHCP, RFC 2138 — RADIUS, RFC 2233 - IF MIB v3, RFC 2373 - IPv6 Aggrega-table 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.

Студия «Проектирования и дизайна сетевых архитектур и инженерной графики», оснащенная в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

– Автоматизированные рабочие места на 12-15 обучающихся с конфигурацией: Core i3 или аналог, дискретная видеокарта, не менее 8GB ОЗУ, один или два монитора 23", мышь, клавиатура;

– Автоматизированное рабочее место преподавателя с конфигурацией: Core i5 или аналог, дискретная видеокарта, не менее 8GB ОЗУ, один или два монитора 23", мышь, клавиатура;

– Специализированная эргономичная мебель для работы за компьютером;

– Офисный мольберт (флипчарт);

– Проектор и экран;

– Маркерная доска;

– Принтер А3, цветной;

– Программное обеспечение общего и профессионального назначения.

Оснащенные базы практики, в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

4.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Баранчиков А.И., Баранчиков П.А., Громов А.Ю. Организация сетевого администрирования 2017 ОИЦ «Академия»

Интернет ресурсы:

6. Гарант. Информационно-правовой портал [Электронный ресурс] : сайт. – Режим доступа: http://www.garant.ru.

7. Электронно-библиотечная система BOOK.ru [Электронный ресурс]: сайт. – Режим доступа: http://www.book.ru.

8. Российская государственная библиотека [Электронный ресурс] / Центр информ. Технологий РГБ ; ред. Власенко Т.В. ; Web-мастер Козлова Н.В. – Электрон.дан. – М. : Рос.гос. б-ка. – Режим доступа: http://www.rsl.ru.

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

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 2.1. Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 2.2. Администрировать сетевые ресурсы в информационных системах.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

ПК 2. 3. Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам
ПК 2.4. Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен/зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	– обоснованность постановки цели, выбора и применения методов и способов решения профессиональных задач; - адекватная оценка и самооценка эффективности и качества выполнения профессиональных задач	Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной
ОК 02.	Осуществлять поиск, анализ и	- использование различных источников, включая электронные ресурсы, медиаресурсы, Интернет-ресурсы, периодические издания по специальности	

	интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	для решения профессиональных задач	программы Экспертное наблюдение и оценка на лабораторно - практических занятиях, при выполнении работ по учебной и производственной практикам Экзамен квалификационный
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.	- демонстрация ответственности за принятые решения - обоснованность самоанализа и коррекция результатов собственной работы;	
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.	- взаимодействие с обучающимися, преподавателями и мастерами в ходе обучения, с руководителями учебной и производственной практик; - обоснованность анализа работы членов команды (подчиненных)	
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	-грамотность устной и письменной речи, - ясность формулирования и изложения мыслей	
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать	- соблюдение норм поведения во время учебных занятий и прохождения учебной и производственной практик,	

	осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.		
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.	- эффективность выполнения правил ТБ во время учебных занятий, при прохождении учебной и производственной практик; - знание и использование ресурсосберегающих технологий в области телекоммуникаций	
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- эффективно использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержание необходимого уровня физической подготовленности.;	
ОК 09.	Использовать информационные технологии в профессиональной	- эффективность использования информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	

	деятельности		
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.	- 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 планировать предпринимательскую деятельность в профессиональной сфере при проведении работ по конструированию сетевой инфраструктуры	

Приложение 2А

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПМ 02. Организация сетевого администрирования

Специальность: 09.02.06 Сетевое и системное администрирование

2020

СОДЕРЖАНИЕ

1.Пояснительная записка

Фонд оценочных средств по профессиональному модулю Организация сетевого администрирования разработан на основании требований ФГОС СПО, с учетом профессиональной направленности программ среднего профессионального образования.

Основная цель создания фонда оценочных средств профессионального модуля – совершенствование содержания профессионального модуля для формирования профессионально - значимых компетенций. Фонд оценочных средств представлен комплектом контрольно-оценочных средств.

ФОС состоит из оценочных средств для: текущего контроля, рубежного контроля и промежуточной аттестации обучающихся.

2.Описание контрольно-оценочных средств

Фонд оценочных средств для текущего, рубежного контроля и промежуточной аттестации разработан для оценки уровня освоения обучающимися планируемых результатов. В ФОС раскрыта типология оценочных ситуаций и заданий текущего, рубежного контроля и промежуточной аттестации, по итогам освоения разделов основного содержания профессионального модуля.

Структурные элементы ФОС по профессиональному модулю:

- результаты освоения ПМ, подлежащие проверке;
- описание контрольно-оценочных средств;
- разноформатные задания для текущего контроля по ПМ;
- разноформатные задания для рубежного контроля по ПМ;
- разноформатные задания для промежуточной аттестации по ПМ.

Кроме оценочных заданий, ФОС включает эталоны ответов к некоторым заданиям, а к типовым – алгоритмы решения либо ориентировочную основу действий.

2.1 Планируемые результаты освоения ПМ 02. Организация сетевого администрирования

Планируемые результаты освоения профессионального модуля в соответствии с ФГОС СПО

Таблица 1

Код ПК, ОК	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	администрировать локальные вычислительные сети; принимать меры по устранению возможных сбоев; обеспечивать защиту при подключении к информационно-телекоммуникационной сети "Интернет".	основные направления администрирования компьютерных сетей; утилиты, функции, удаленное управление сервером; технологию безопасности, протоколов
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.		
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.		
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с		

коллегами, руководством, клиентами.		авторизации, конфиденциальности и безопасности при работе с сетевыми ресурсами.
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.		
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.		
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности		
ОК 09. 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.		
ПК 2.1 Администрировать локальные вычислительные сети и принимать меры по устранению возможных сбоев.		
ПК 2.2 Администрировать сетевые ресурсы в информационных системах.		
ПК 2.3 Обеспечивать сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей		
ПК 2.4 Взаимодействовать со специалистами смежного профиля при разработке методов, средств и технологий применения объектов профессиональной деятельности.		

3.Фонды оценочных средств

3.1 Фонд оценочных средств для текущего контроля

Текущий контроль проводится во время аудиторных занятий по ПМ

Организация сетевого администрирования в соответствии с учебным планом и рабочей программы ПМ 02. Организация сетевого администрирования

ТЕМА 1.1 УСТАНОВКА И НАСТРОЙКА WINDOWS SERVER 2012 R2

Устный опрос по теме «Установка и настройка Windows Server 2012 R2»

Вопросы:

1. Развертывание и управление Windows Server 2012 R2.
2. Управление объектами доменных служб Службы Каталога
3. Применение протокола DHCP
4. Применение DNS.
5. Применение групповой политики

Оценивание: при оценивании ответов учитываются следующие критерии:

1. точность ответа;
2. полнота ответа;
3. логичность и последовательность высказывания;
4. ответы на дополнительные вопросы по теме.

ТЕМА 1.2 ЭКСПЛУАТАЦИЯ ТЕХНИЧЕСКИХ СРЕДСТВ СЕТЕВОЙ ИНФРАСТРУКТУРЫ

Практическая работа №1 Настройка и устранение неполадок службы DNS

Цель работы:

Практическое применение полученных на теоретических занятиях знаний, приобретение практических умений и навыков.

Краткое описание

Имеется виртуальная машина с установленной ОС Linux, в Linux установлен DNS-сервер (семейство пакетов bind). Требуется настроить DNS-сервер для поддержки некоторого множества зон и записей ресурсов.

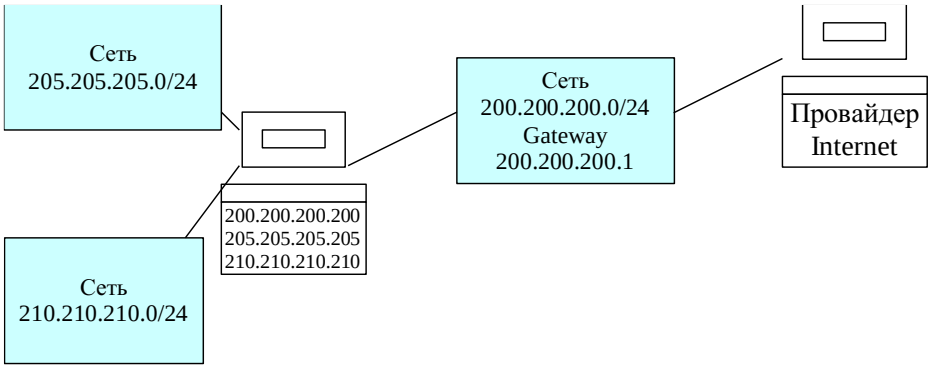
Постановка задачи

Вам предоставлена виртуальная машина, которую нужно настроить для работы в качестве сервера DNS.

1. Существенные элементы конфигурации виртуальной машины.

- **имеет сетевую плату AMD PCNet PCI Adapter;**
- **установленная операционная система – Linux;**
- **параметры TCP/IP, назначенные сетевой плате, следующие:**
  - **eth0 – 205.205.205.254/24,gateway 205.205.205.205**
- **установленные сетевые протоколы – TCP/IP;**
- **установлен сервер DNS;**
- **имеется учетная запись пользователя root, пароль rootroot.**

2. Топология сети и адреса



Требуется настроить сервер DNS таким образом, чтобы удовлетворялись следующие условия:

- **Данный DNS сервер**
  - **Является основным DNS-сервером для домена «aaa.ru.»**
  - **Является основным DNS-сервером для домена «bbb.ru.»**
  - **Является основным DNS-сервером для домена «aaa.bbb.ru.»**
  - **Является подчиненным DNS-сервером для домена «ccc.ru.», IP-адрес основного DNS-сервера данного домена – 190.190.190.190**
  - **Делегирует полномочия по управлению доменом «child.bbb.ru.» DNS-серверу с IP-адресом 210.210.210.210**
  - **Делегирует полномочия по управлению доменом «child.aaa.ru.» DNS-серверу с IP-адресом 220.220.220.220**
- **Ниже перечислены имена узлов, имеющих различные IP-адреса**
  - **210.210.210.10 – www.aaa.ru., www.bbb.ru., www.aaa.bbb.ru.**
  - **210.210.210.20 – ftp.aaa.ru., ftp.bbb.ru., ftp.aaa.bbb.ru., mail1.bbb.ru., является вторым почтовым сервером домена «bbb.ru.»**
  - **210.210.210.30 – mail.aaa.ru., mail.bbb.ru., mail.aaa.bbb.ru. – является первым почтовым сервером доменов «aaa.ru.», «bbb.ru.», «aaa.bbb.ru.»**
  - **205.205.205.10 – ns2.aaa.ru., ns2.bbb.ru., ns2.aaa.bbb.ru. – является подчиненным сервером DNS доменов «aaa.ru.», «bbb.ru.», «aaa.bbb.ru.».**
  - **205.205.205.20 – mail1.aaa.ru., mail1.aaa.bbb.ru. – является вторым почтовым сервером доменов «aaa.ru.», «aaa.bbb.ru.»**
  - **205.205.205.30 – trash.aaa.ru.**
  - **220.220.220.220 –mail2.bbb.ru., mail2.aaa.ru., mail2.aaa.bbb.ru. - является третьим почтовым сервером доменов «aaa.ru.», «bbb.ru.», «aaa.bbb.ru.»**
  - **Требуется добавить 5 машин с произвольными IP-адресами из сетей 210.210.210.0/24 и 205.205.205.0/24 и произвольными именами в доменах «aaa.ru.», «bbb.ru.», «aaa.bbb.ru.» (должны присутствовать имена из всех доменов и адреса из всех сетей).**

Дополнительная информация

Настройка производится посредством редактирования основного конфигурационного файла /etc/named.conf и файлов зон (их размещение указывается в основном конфигурационном файле)

- **Перезапуск DNS-сервера производится командой**
  - **service named restart**
- **Справку по структуре файла /etc/named.conf можно посмотреть, выполнив команду**
  - **man named.conf (для выхода из просмотра нажмите кнопку "q")**
- **Перезагрузку Linux можно выполнить командой**
  - **shutdown –r now**
- **Выключить Linux можно командой**
  - **shutdown –h now**

Оценивание практических работ:
5(отлично) – работа выполнена полностью, все действия выполнены верно.
4 (хорошо) – работа выполнена не полностью, верно решено 80% задания.
3 (удовлетворительно) – работа выполнена не полностью, верно решено 70% задания.
2 (неудовлетворительно) – работа выполнена не полностью, верно решено менее 60% задания.

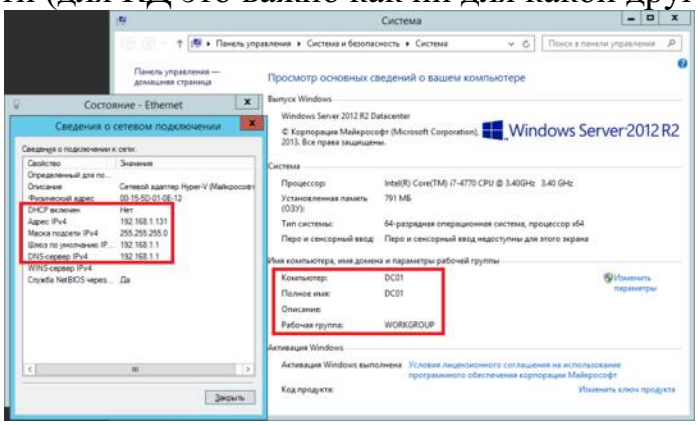
Практическая работа №2 Поддержка ADDS

Цель работы:
Практическое применение полученных на теоретических занятиях знаний, приобретение практических умений и навыков.

Подготовка окружения

Разворачивать роль AD планирую на двух виртуальных серверах (будущих контроллерах домена) по очереди.

1. Первым делом нужно задать подходящие **имена серверов**, у меня это будут DC01 и DC02;
2. Далее прописать **статические настройки сети** (подробно этот момент я рассмотрю ниже);
3. Установите **все обновления системы**, особенно обновления безопасности (для КД это важно как ни для какой другой роли).

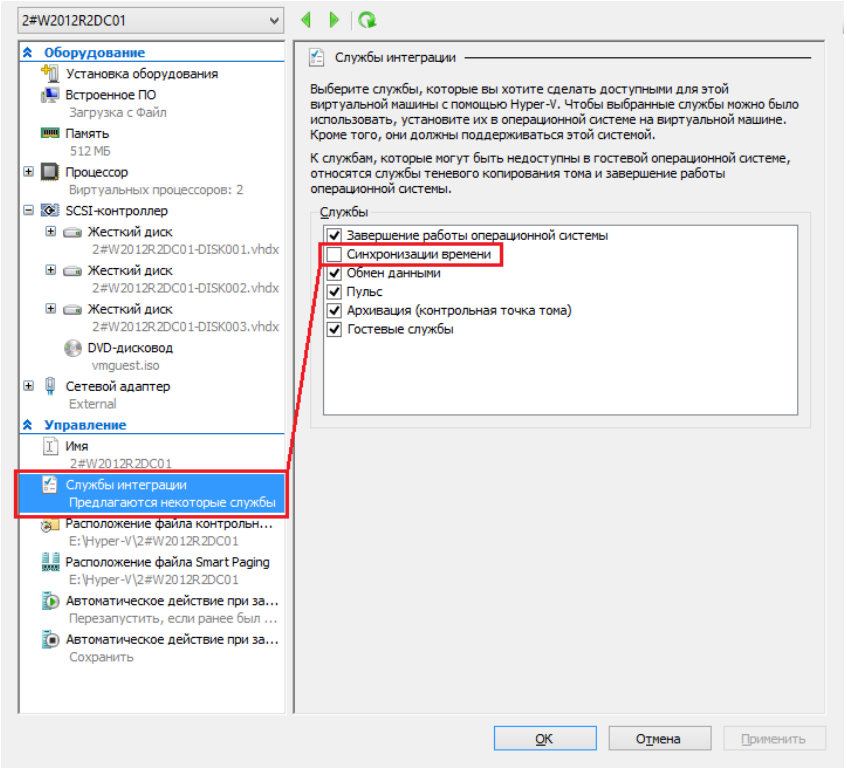


На этом этапе необходимо определиться **какое имя домена у вас будет**. Это крайне важно, поскольку потом смена доменного имени будет очень

большой проблемой для вас, хоть и сценарий переименования официально поддерживается и внедрен достаточно давно.

Примечание: *некоторые рассуждения, а также множество ссылок на полезный материал, вы можете найти в моей статье Пара слов про именование доменов Active Directory. Рекомендую ознакомиться с ней, а также со списком использованных источников.*

Поскольку у меня будут использоваться виртуализованные контроллеры домена, необходимо изменить некоторые настройки виртуальных машин, а именно **отключить синхронизацию времени с гипервизором**. Время в AD должно синхронизироваться исключительно с внешних источников. Включенные настройки синхронизации времени с гипервизором могут обернуться циклической синхронизацией и как следствие проблемами с работой всего домена.



Примечание: *отключение синхронизации с хостом виртуализации — самый простой и быстрый вариант. Тем не менее, это не best practic. Согласно рекомендациям Microsoft, нужно отключать синхронизацию с хостом лишь частично [1]. Для понимания принципа работы читайте официальную документацию [2] [3], которая в последние годы радикально подскочила вверх по уровню изложения материала.*

Вообще сам подход к администрированию виртуализованных контроллеров домена отличается в виду некоторых особенностей функционирования AD DS [4] [5]:

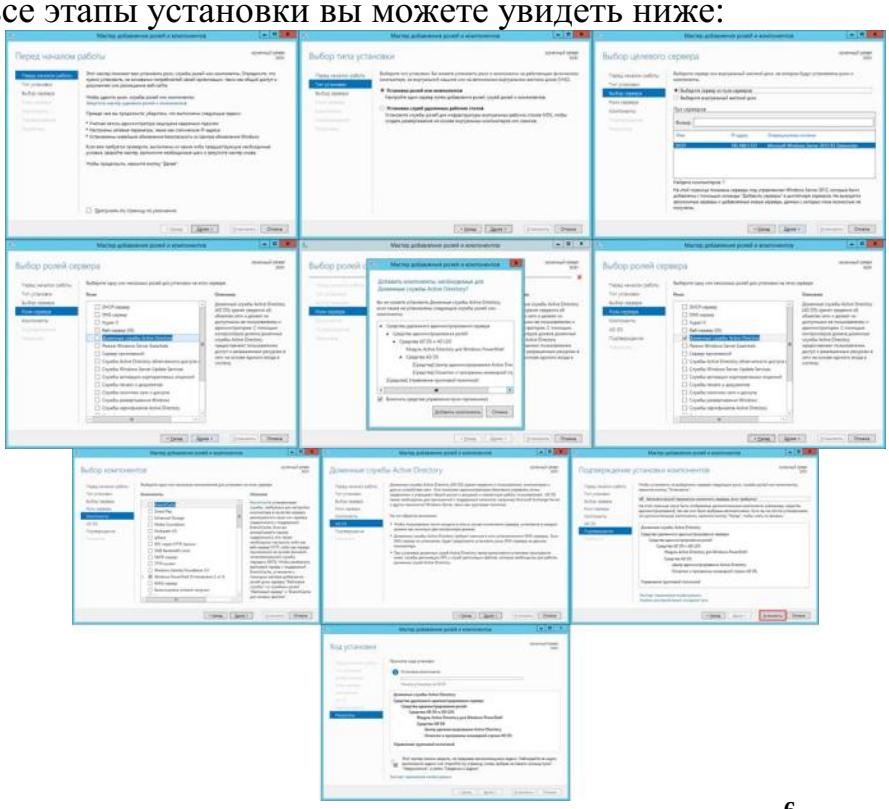
Виртуальные среды представляют особую трудность для распределенных рабочих потоков, зависящих от логической схемы репликации по времени. Например, репликация AD DS использует равномерно увеличивающееся значение (которое называется USN, или номер последовательного обновления), назначенное транзакциям в каждом контроллере домена.

Каждый экземпляр базы данных контроллера домена также получает идентификатор под названием InvocationID. InvocationID контроллера домена и его номер последовательного обновления вместе служат уникальным идентификатором, который связан с каждой транзакцией записи, выполняемой на каждом контроллере домена, и должны быть уникальны в пределах леса.

На этом основные шаги по подготовке окружения завершены, переходим к этапу установки.

Установка Active Directory

Установка производится через Server Manager и в ней нет ничего сложного, подробно все этапы установки вы можете увидеть ниже:



Сам процесс установки претерпел некоторые изменения [6] по сравнению с предыдущими версиями ОС:

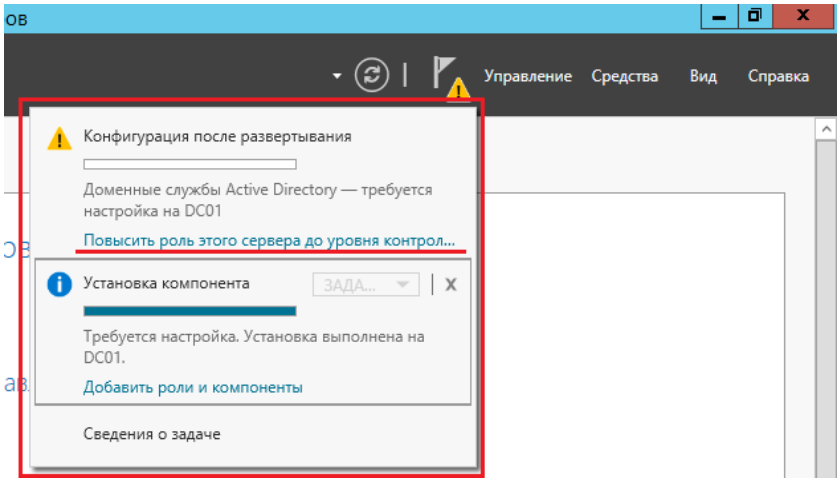
Развертывание доменных служб Active Directory (AD DS) в Windows Server 2012 стало проще и быстрее по сравнению с предыдущими версиями Windows Server. Установка AD DS теперь выполняется на основе Windows PowerShell и интегрирована с диспетчером серверов. Сократилось количество шагов, необходимых для внедрения контроллеров домена в существующую среду Active Directory.

Необходимо выбрать только роль *Доменные службы Active Directory*, никакие дополнительные компоненты устанавливать не нужно. Процесс установки занимает незначительно время и можно сразу переходить к настройке.

Настройка Active Directory

Когда установится роль, справа вверху Server Manager вы увидите восклицательный знак — требуется провести конфигурацию после

развертывания. Нажимаем *Повысить роль этого сервера до контроллера домена*.

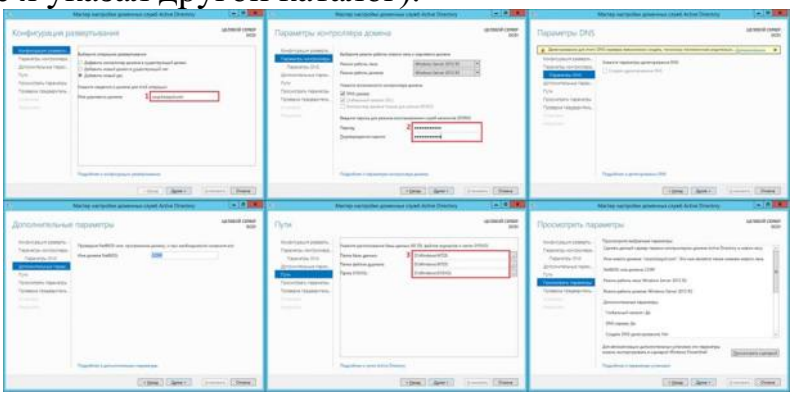


Далее весь процесс будет проходить в мастере настройки.

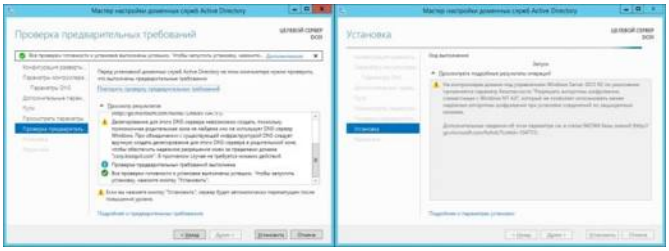
Повышение роли сервера до контроллера домена

Этапы работы мастера подробно описаны в документации [7]. Тем не менее, пройдемся по основным шагам.

Поскольку мы разворачиваем AD с нуля, то нужно добавлять новый лес. Не забудьте надежно сохранить пароль для режима восстановления служб каталогов (DSRM). Расположение базы данных AD DS можно оставить по умолчанию (именно так и рекомендуют. Однако для разнообразия в своей тестовой среде я указал другой каталог).



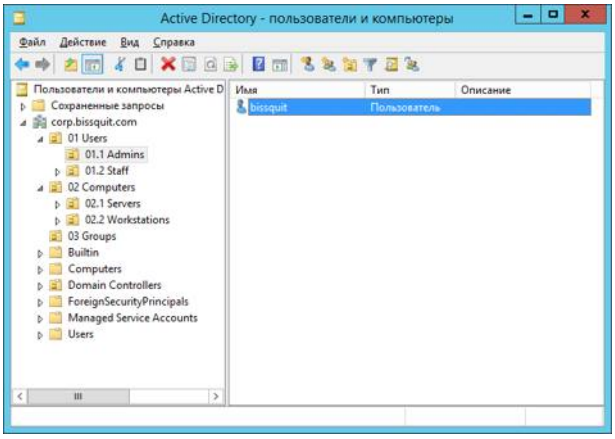
Дожидаемся установки.



После этого сервер самостоятельно перезагрузится.

Создание учетных записей администраторов домена/предприятия

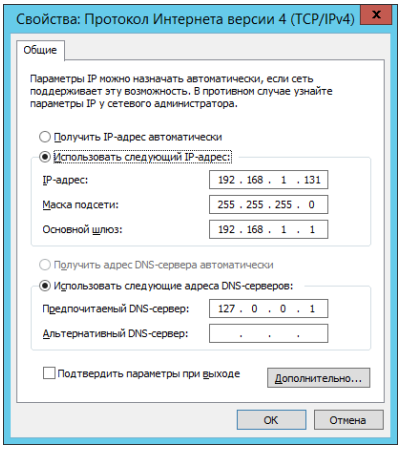
Залогиниться нужно будет под учетной записью локального администратора, как и прежде. Зайдите в оснастку *Active Directory — пользователи и компьютеры*, создайте необходимые учетные записи — на этом этапе это администратор домена.



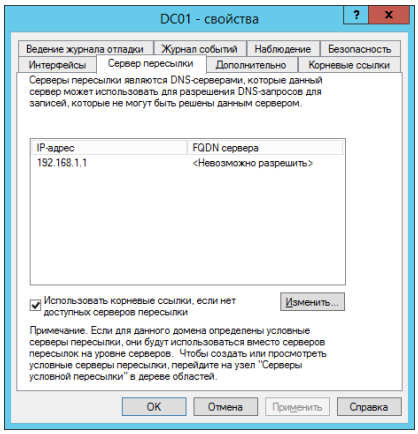
Сразу же рекомендую настроить и иерархию организации (только не используйте русские символы!).

Настройка DNS на единственном DC в домене

Во время установки AD также была установлена роль AD DNS, поскольку других серверов DNS у меня в инфраструктуре не было. Для правильно работы сервиса необходимо изменить некоторые настройки. Для начала нужно проверить предпочитаемые серверы DNS в настройках сетевого адаптера. Необходимо использовать только один DNS-сервер с адресом 127.0.0.1. Да, именно localhost. По умолчанию он должен прописаться самостоятельно.



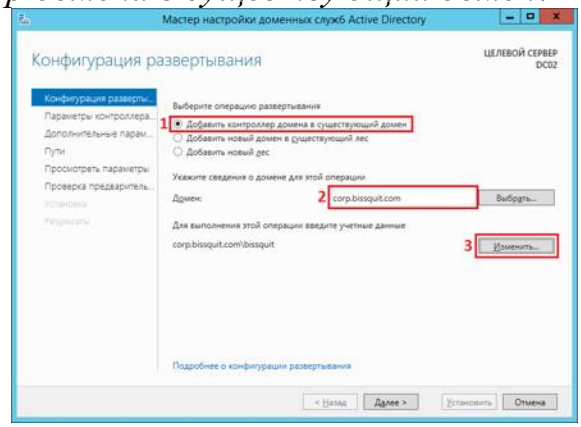
Убедившись в корректности настроек, открываем оснастку DNS. Правой кнопкой нажимаем на имени сервера и открываем его свойства, переходим на вкладку «Сервер пересылки». Адрес DNS-сервера, который был указан в настройках сети до установки роли AD DS, автоматически прописался в качестве единственного сервера пересылки:



Необходимо его удалить и создать новый и крайне желательно, чтобы это был сервер провайдера, но никак не публичный адрес типа общеизвестных 8.8.8.8 и 8.8.4.4. Для отказоустойчивости пропишите минимум два сервера. Не снимайте галочку для использования корневых ссылок, если нет доступных серверов пересылки. Корневые ссылки — это общеизвестный пул DNS-серверов высшего уровня.

Добавление второго DC в домен

Поскольку изначально я говорил о том, что у меня будет два контроллера домена, пришло время заняться настройкой второго. Проходим также мастер установки, повышаем роль до контроллера домена, только выбираем *Добавить контроллер домена в существующий домен*:

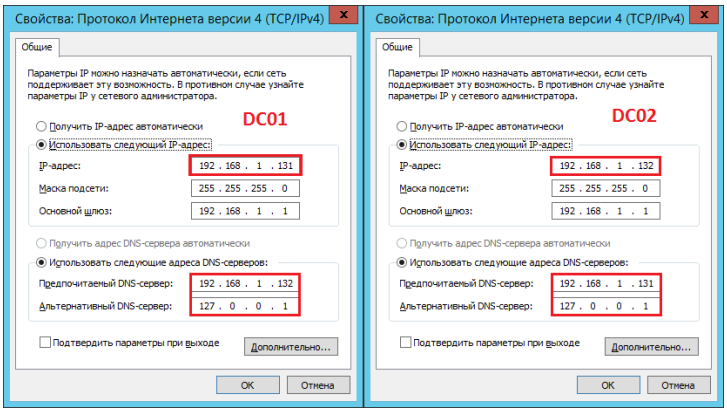


Обратите внимание, что в сетевых настройках этого сервера основным **DNS-сервером должен быть выбран настроенный ранее первый контроллер домена**! Это обязательно, иначе получите ошибку.

После необходимых настроек логиньтесь на сервер под учетной записью администратора домена, которая была создана ранее.

Настройка DNS на нескольких DC в домене

Для предупреждения проблем с репликацией нужно снова изменить настройки сети и делать это необходимо на каждом контроллере домена (и на существовавших ранее тоже) и каждый раз при добавлении нового DC:



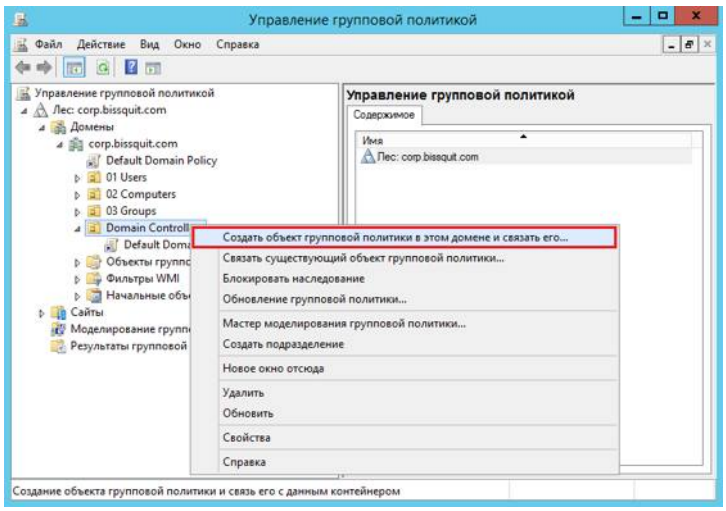
Если у вас больше трех DC в домене, необходимо прописать DNS-серверы через дополнительные настройки именно в таком порядке. Подробнее про DNS вы можете прочитать в моей статье Шпаргалка по DNS.

Настройка времени

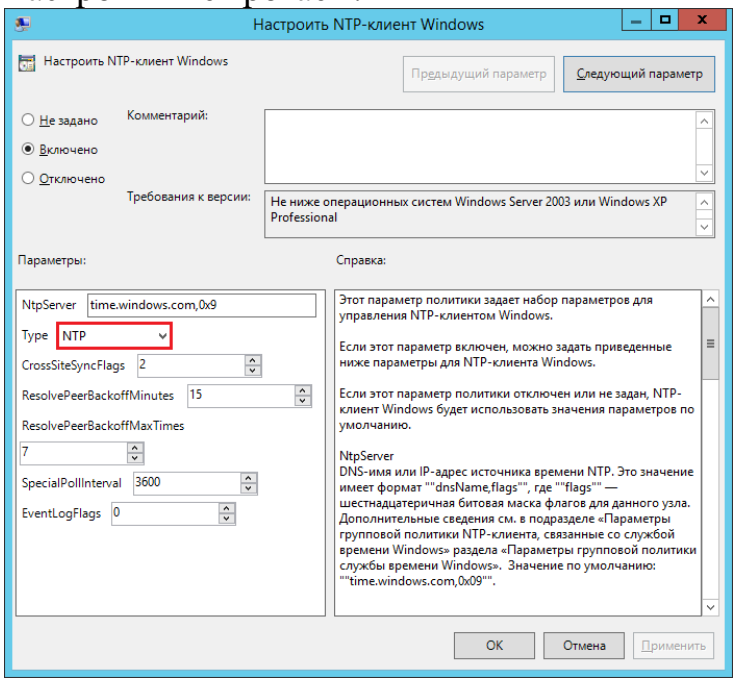
Этот этап нужно выполнить обязательно, особенно если вы настраиваете реальное окружение в продакшене. Как вы помните, ранее я отключил синхронизацию времени через гипервизор и теперь нужно её настроить должным образом. За распространение правильного время на весь домен отвечает контроллер с ролью FSMO PDC эмулятор). В моем случае это конечно же первый контроллер домена, который и является носителем всех ролей FSMO изначально.

```
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\bissquit>w32tm /query /status
Индикатор помех: 0(предупреждений нет)
Страта: 1 (основная ссылка - синхронизирована по радиочасам)
Точность: -6 (15.625ms за такт времени)
Задержка корня: 0.0000000s
Дисперсия корня: 10.0000000s
Идентификатор опорного времени: 0x4C4F434C (имя источника:  "LOCL")
Время последней успешной синхронизации: 16.03.2016 8:20:12
Источник: Local CMOS Clock
Интервал опроса: 6 (64s)

C:\Users\bissquit>_
```

Настраивать время на контроллерах домена будем с помощью групповых политик. Напоминаю, что учетные записи компьютеров контроллеров домена находятся в отдельном контейнере и имеют отдельную групповую политику по умолчанию. Не нужно вносить изменения в эту политику, лучше создайте новую.



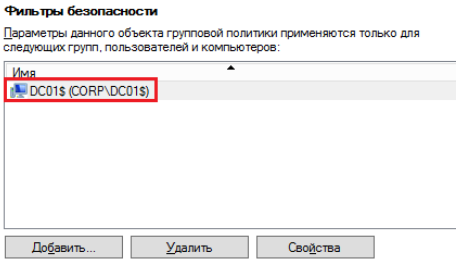
Назовите её как считаете нужным и как объект будет создан, нажмите правой кнопкой — *Изменить*. Переходим в *Конфигурация компьютера\Политики\Административные шаблоны\Система\Служба времени Windows\Поставщики времени*. Активируем политики *Включить NTP-клиент Windows* и *Включить NTP-сервер* Windows, заходим в свойства политики *Настроить NTP-клиент Windows* и выставляем тип протокола — *NTP*, остальные настройки не трогаем:



Дожидаемся применения политик (у меня это заняло примерно 5-8 минут, несмотря на выполнение gpupdate /force и пару перезагрузок), после чего получаем:

```
Microsoft Windows [Version 6.3.9600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2013. Все права защищены.

C:\Users\bissquit>w32tm /query /status
Индикатор помех: 0(предупреждений нет)
Страта: 4 (вторичная ссылка - синхронизирована с помощью (S)NTP)
Точность: -6 (15.625ms за такт времени)
Задержка корня: 0.0645941s
Дисперсия корня: 7.8801017s
Идентификатор опорного времени: 0xBFE95169 (IP-адрес источника:  191.233.81.105)

Время последней успешной синхронизации: 16.03.2016 8:51:19
Источник: time.windows.com,0x9
Интервал опроса: 6 (64s)

C:\Users\bissquit>_
```

Вообще надо сделать так, чтобы время с внешних источников синхронизировал только PDC эмулятор, а не все контроллеры домена под ряд, а будет именно так, поскольку групповая политика применяется ко всем объектам в контейнере. Нужно её перенаправить на конкретный объект учетной записи компьютера-владельца роли PDC-эмулятор. Делается это также через групповые политики — в консоли gpmc.msc нажимаем левой кнопкой нужную политику и справа у вас появятся её настройки. В фильтрах безопасности нужно добавить учетную запись нужного контроллера домена:



Оценивание практических работ:
5(отлично) – работа выполнена полностью, все действия выполнены верно.
4 (хорошо) – работа выполнена не полностью, верно решено 80% задания.
3 (удовлетворительно) – работа выполнена не полностью, верно решено 70% задания.
2 (неудовлетворительно) – работа выполнена не полностью, верно решено менее 60% задания.

Практическая работа №3 Управление пользовательскими и служебными учетными записями

Цель работы:
Практическое применение полученных на теоретических занятиях знаний, приобретение практических умений и навыков.
Ход работы 1. Управление учётными записями локальных пользователей
Выберите пункт «Управление» в контекстном меню «Моего компьютера».
Выберите «Локальные пользователи и группы» (рис. 1).

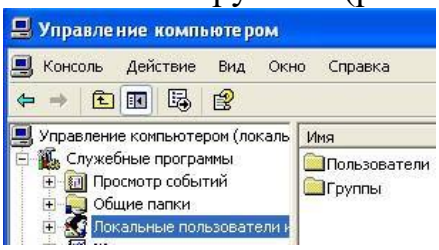


Рисунок 1 – Управление компьютером

Для создания новой учётной записи в контекстном меню раздела «Пользователи», расположенного в правой части окна, (или в меню «Действие») и выберите пункт «Новый пользователь» (рис. 2).

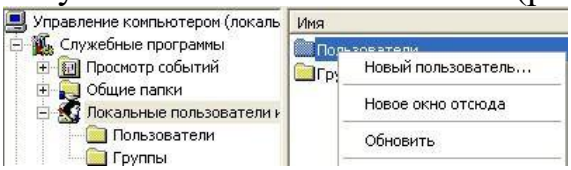


Рисунок 2 – Создание учётной записи

В появившемся окне (рис. 3) введите имя учётной записи, а также пароль и его подтверждение. Если администратор устанавливает пользователю временный пароль, то для обязательной смены пароля необходимо включить параметр «Потребовать смену пароля при следующем входе в систему». Сразу после успешной аутентификации пользователь получает

запрос на смену пароля, в ответ на который он должен задать новый пароль. Этот подход необходимо использовать в тех случаях, когда администратор системы не должен знать пароли пользователей.

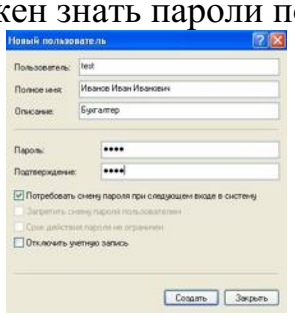


Рисунок 3 – Настройка параметров учётной записи при её создании

Если пользователь забыл свой пароль, то член группы «Администраторы» может сбросить его старый пароль при помощи функции «Задать пароль», доступной в контекстном меню учётной записи этого пользователя (рис. 4). Смените пароль у созданной учётной записи.

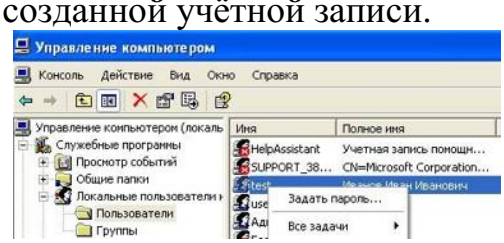


Рисунок 4 – Функция «Задать пароль»

Войдите в систему под созданной учётной записью. При первом входе пользователю будет выдано сообщение о необходимости ввести пароль (рис. 5) и окно смены пароля (рис. 6). Смените пароль созданной учётной записи.

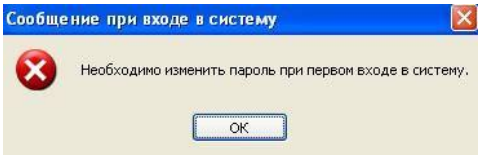


Рисунок 5 – Сообщение пользователю о необходимости смены пароля

Для применения к пользователю набора прав и ограничений можно включить его учётную запись в группу пользователей с соответствующим набором прав и ограничений.

Войдите в систему под учётной записью «Администратор». Откройте «Свойства» созданной учётной записи. На вкладке «Членство в группах» добавьте пользователя в группу «Опытные пользователи» (рис. 7). Имя группы можно ввести самостоятельно или выбрать из списка, предоставляемого после последовательного нажатия кнопок «Дополнительно» и «Поиск».

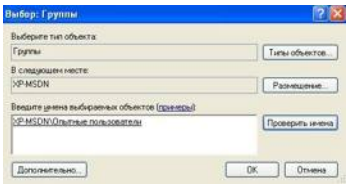


Рисунок 7 – Добавление пользователя в группу

В разделе «Группы» откройте «Свойства» группы «Опытные пользователи» и проверьте наличие в группе добавленной учётной записи. Создайте новую группу и добавьте в неё этого же пользователя (рис. 8).

Настройка политики учётной записи

Откройте «Локальную политику безопасности» («Пуск – Панель управления – Администрирование – Локальная политика безопасности»). Основное окно «Локальной политики безопасности» представлено на рис. 9. Значения параметров, заданные при настройке политики, будут применяться ко всем пользователям локального компьютера.

Раздел «Политики учётных записей» «Локальной политики безопасности» включает в себя настройки, применяющиеся к паролям пользователей.

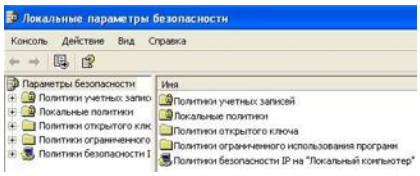


Рисунок 9 – Локальная политика безопасности

Выберите раздел «Политика паролей» («Параметры безопасности – Политики учётных записей – Политика паролей»). Настройки, входящие в раздел «Политика паролей», представлены на рис. 10.

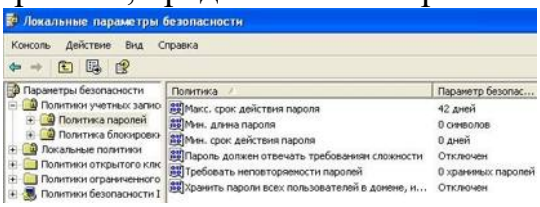


Рисунок 10 – Параметры раздела «Политика паролей»

Установите максимальный срок действия пароля – 30 дней.

Установите минимальную длину пароля – 10 символов.

Для параметра «Требовать неповторяемости паролей» (рис. 11) установите значение 3 хранимых пароля, означающее, что новый пароль должен отличаться от 3 последних паролей пользователя. Включите параметр «Пароль должен отвечать требованиям сложности» (рис. 12).

Параметр «Пароль должен отвечать требованиям сложности» определяет требования сложности для паролей. Если эта политика включена, то пароли должны удовлетворять следующим минимальным требованиям:

пароль не может содержать имя учётной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из шести символов;
в пароле должны присутствовать символы трёх категорий из числа следующих четырёх:
а) прописные буквы английского алфавита от A до Z;
б) строчные буквы английского алфавита от a до z;
в) десятичные цифры (от 0 до 9);
г) неалфавитные символы (например, !, $, #, %).
Проверка соблюдения этих требований выполняется при изменении или создании паролей. При помощи этого параметра можно избавиться от легко подбираемых паролей типа «111», «qwerty», «12345» и т. д.

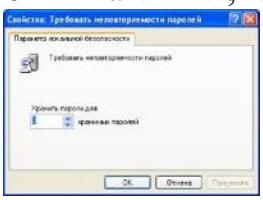


Рисунок 11 – Параметр «Требовать неповторяемости паролей»

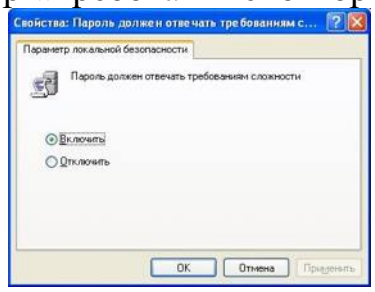


Рисунок 12 – Параметр «Пароль должен отвечать требованиям сложности»

Переведите системное время более чем на 30 дней вперёд. Попытайтесь войти под созданной учётной записью. Пользователю будет выдано сообщение об истечении срока действия пароля (рис. 13). При смене пароля попытайтесь заменить пароль на более простой (например, abc12345 или включающий имя учётной записи). В этом случае пользователю будет выдано сообщение об ошибке при смене пароля (рис. 14). Введите пароль удовлетворяющий требованиям.

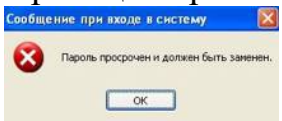


Рисунок 13 – Сообщение об истечении срока действия пароля

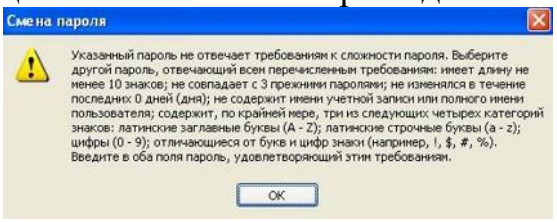


Рисунок 14 – Сообщение о недостаточном качестве нового пароля

Войдите в систему под учётной записью «Администратор». Переведите системное время в исходное состояние. Выберите раздел «Политика блокировки учётной записи» («Параметры безопасности – Политики

учётных записей – Политика блокировки учётной записи»). Настройки, входящие в раздел «Политика блокировки учётной записи», представлены на рис. 15.

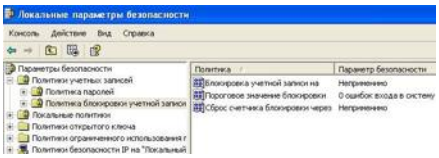


Рисунок 15 – Параметры раздела «Политика блокировки учётной записи»

Настройте параметры следующим образом:
установить пороговое значение блокировки, равное 3 ошибкам входа в систему (после 3 неудачных попыток входа учётная запись блокируется, рис. 16);
установить длительность блокировки в параметре «Блокировка учётной записи на», равную 30 мин (значение 0 означает, что блокировку может снять только администратор);

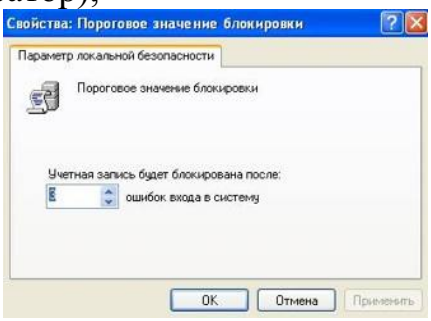


Рисунок 16 – Параметр «Пороговое значение блокировки»
установите сброс счётчика блокировки через 15 мин. Если в течение установленного времени будет 3 неудачных попытки входа, то учётная запись блокируется. Если неудачных попыток в течение установленного времени будет меньше, то опять допускается 3 неудачных попытки (значение этого параметра не должно превышать длительность блокировки учётной записи).
Завершите сеанс учётной записи «Администратор». При входе с систему под созданной учётной записью три раза введите неправильный пароль. При следующей попытке входа в систему будет выдано сообщение о блокировании созданной учётной записи (рис.
17).

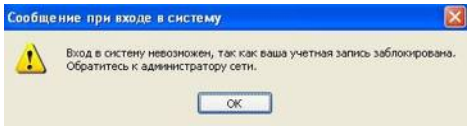


Рисунок 17 – Сообщение о блокировании учётной записи
Войдите в систему под учётной записью «Администратор». Разблокируйте созданную учётную запись. Для этого в окне
«Свойства» этой учётной записи («Управление компьютером – Локальные пользователи и группы – Пользователи», рис. 18) отключите настройку «Заблокировать учётную запись».

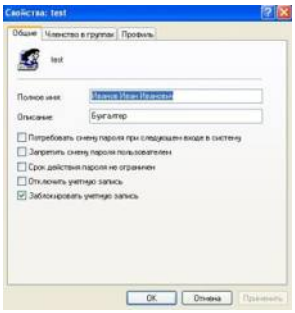


Рисунок 18 – Свойства заблокированной учётной записи

Настройка прав пользователей

Раздел «Назначение прав пользователей» включает набор привилегий, которыми можно наделять пользователей или группы пользователей (примеры привилегий: архивирование и восстановление файлов и каталогов, загрузка и выгрузка драйверов устройств, изменение системного времени).

Выберите раздел «Назначение прав пользователя» («Параметры безопасности – Локальные политики – Назначение прав пользователя», рис. 19).

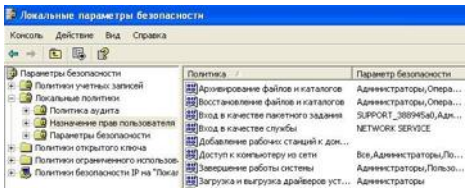


Рисунок 19 –Раздел «Назначение прав пользователя»

Присвоение права «Завершение работы системы»:

в свойствах выбранного параметра (рис. 20) удалите все группы, кроме группы «Администраторы»;

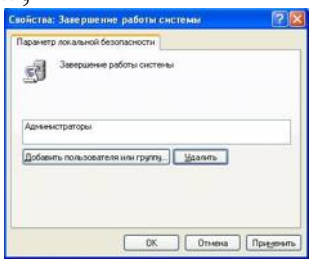


Рисунок 20 – Настройка параметра «Завершение работы системы»

нажмите кнопку «Добавить пользователя или группу»;

нажмите кнопку «Типы объектов» и добавьте в параметры поиска тип «Группы»;

выберите созданную группу (рис. 21).

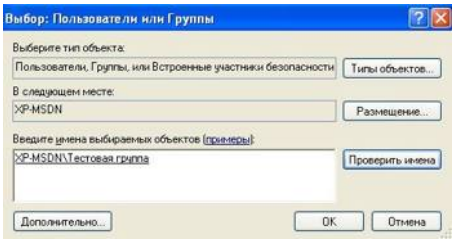


Рисунок 21 – Выбор пользователя или группы пользователей

Таким образом, пользователи, входящие в выбранную группу, в дополнение к правам групп «Пользователи» и «Опытные пользователи» получают право на завершение работы системы.

Войдите в систему под созданной учётной записью. Проверьте возможность завершения работы системы этим пользователем. Под учётной записью «Администратор» исключите созданную учётную запись из созданной группы. Повторно проверьте возможность завершения работы системы этим пользователем.

Проверьте возможность изменения системного времени под созданной учётной записью. Под учётной записью «Администратор» выберите параметр «Изменение системного времени» в разделе «Назначение прав пользователя» и в свойствах этого параметра удалите группу «Опытные пользователи». Повторно проверьте возможность изменения системного времени под созданной учётной записью.

Настройка параметров безопасности операционной системы

Раздел «Параметры безопасности» позволяет изменять настройки операционной системы, каким-либо образом влияющие на безопасность: возможности учётной записи «Гость», параметры работы модуля входа в систему и т. д.

Выберите раздел «Параметры безопасности» («Параметры безопасности – Локальные политики – Параметры безопасности», рис. 22).

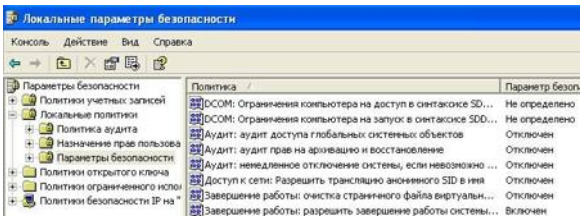


Рисунок 22 – Раздел «Параметры безопасности»

Измените следующие настройки:

применительно к группе настроек «Завершение работы» – отключите параметр «разрешить завершение работы системы без выполнения входа в систему» (рис. 23);

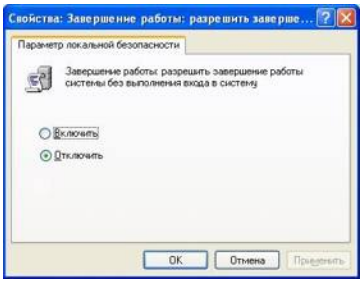


Рисунок 23 – Параметр «Разрешить завершение работы без выполнения входа в систему»

применительно к группе настроек «Интерактивный вход в систему» – включите параметр «не отображать последнего имени пользователя» (рис. 24) и установите значение параметра «напоминать пользователям об истечении срока действия пароля заранее», равным 3 дням;

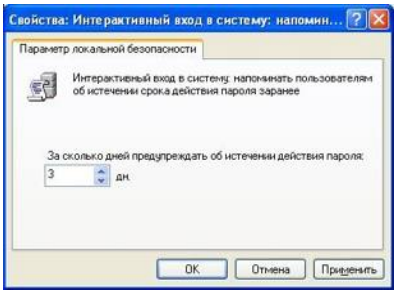


Рисунок 24 – Параметр «Напоминать пользователям об истечении срока действия пароля заранее»

применительно к группе настроек «Интерактивный вход в систему», отключите параметр «не требовать нажатия CTRL+ALT+DEL». Если эта настройка включена, то пользователь не должен для входа в систему нажимать CTRL+ALT+DEL. В таком случае система становится уязвимой для атак, основанных на перехвате паролей пользователей. Если потребовать нажатия клавиш CTRL+ALT+DEL перед входом в систему, то пользователям будет гарантирован надёжно защищенный канал передачи паролей;

применительно к группе настроек «Устройства» – включите параметр «запретить пользователю установку драйверов принтера». Чтобы локальный компьютер мог выполнять печать на сетевом принтере, необходимо установить на компьютере драйвер этого принтера. Данный параметр безопасности определяет, кому при добавлении сетевого принтера разрешается устанавливать драйвер принтера. Если параметр включен, то устанавливать драйвер при добавлении сетевого принтера разрешается только группам «Администраторы» и «Опытные пользователи». Если параметр отключен, то устанавливать драйвер при добавлении сетевого принтера может любой пользователь;

применительно к группе настроек «Устройства» – параметр «разрешено форматировать и извлекать съёмные носители» разрешите группам пользователей «Администраторы», «Опытные пользователи» (рис. 25). Этот параметр безопасности определяет, каким пользователям разрешается форматировать съёмные носители NTFS и извлекать их из устройств;

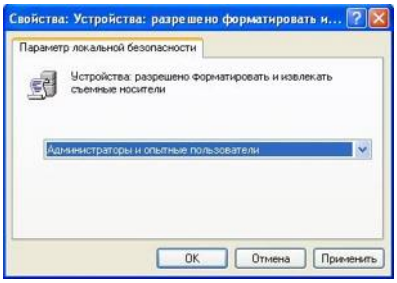


Рисунок 25 – Параметр «Разрешено форматировать и извлекать съёмные носители»

измените параметр «Переименование учётной записи администратора» (рис. 26), переименование учётной записи усложнит пользователям, не

имеющим доступа в систему, процесс угадывания имени пароля пользователя с правами администратора.

Проверьте применение настроек, изменённых в данном разделе: возможность завершения работы без входа в систему, напоминание пользователю об истечении срока действия пароля, необходимость нажатия CTRL+ALT+DEL и отсутствие имени предыдущего пользователя при входе в систему, переименование учётной записи администратора.

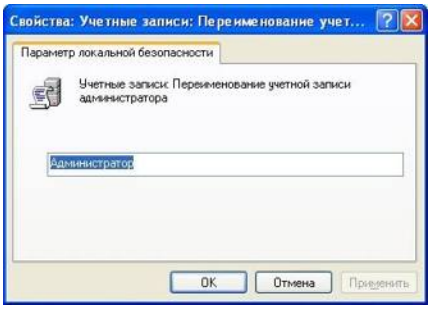


Рисунок 26 – Параметр «Переименование учётной записи администратора»

Задание

1. Создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы.
2. Создайте учётную запись с именем Вашей учётной записи в кафедральной сети и включите её в созданную группу.
3. Примените к созданной учётной записи настройки, указанные в Вашем варианте (табл. 1).

Таблица 1 – Варианты заданий

Параметр \ Вариант	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Пароль должен отвечать требованиям сложности	+	-	-	+	-	-	+	-	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на…	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через…	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	

Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

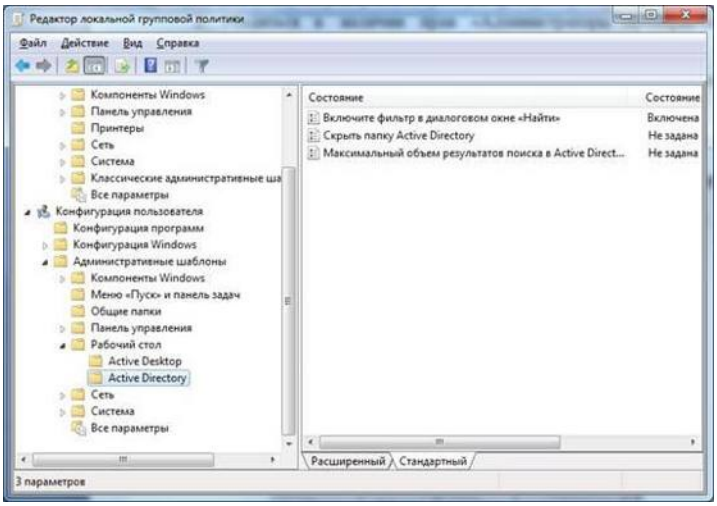
Контрольные вопросы

1. Поясните параметр «Потребовать смену пароля при следующем входе в систему».
2. Включение какого параметра разрешает пользователю не изменять пароль по окончании его действия?
3. Какая функция позволяет сбросить забытый пароль пользователя, и кто может воспользоваться этой функцией?
4. Какой параметр задаёт периодичность смены пароля?
5. Поясните параметр «Требовать неповторяемости паролей».
6. Поясните параметр «Пароль должен отвечать требованиям сложности» и перечислите минимальные требования, которым должны удовлетворять пароли, если параметр включен.
7. Какие параметры входят в политику блокировки учётной записи?
8. Возможно ли, что учётная запись не будет блокирована при количестве ошибок большем, чем установленное пороговое значение?
9. В каком разделе предоставляется возможность назначать пользователям права, связанные с информационной безопасностью?
10. В каком разделе предоставляется возможность устанавливать параметры операционной системы, связанные с информационной безопасностью?

Оценивание практических работ:
5(отлично) – работа выполнена полностью, все действия выполнены верно.
4 (хорошо) – работа выполнена не полностью, верно решено 80% задания.
3 (удовлетворительно) – работа выполнена не полностью, верно решено 70% задания.
2 (неудовлетворительно) – работа выполнена не полностью, верно решено менее 60% задания.

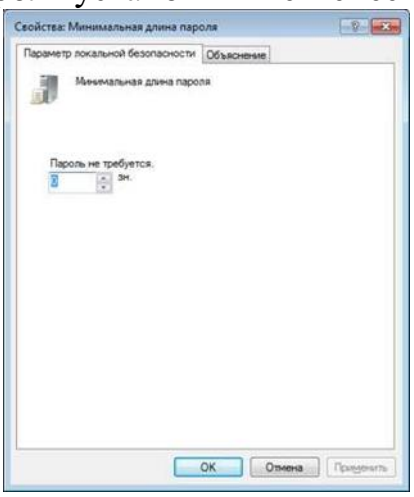
Практическая работа №4 Внедрение инфраструктуры Групповых политик

Цель работы:
Практическое применение полученных на теоретических занятиях знаний, приобретение практических умений и навыков.
Ход работы:
«Пуск» - «Выполнить». В появившемся окне ввести команду «gpedit.msc» для вывода на экран консоли «Active Directory"

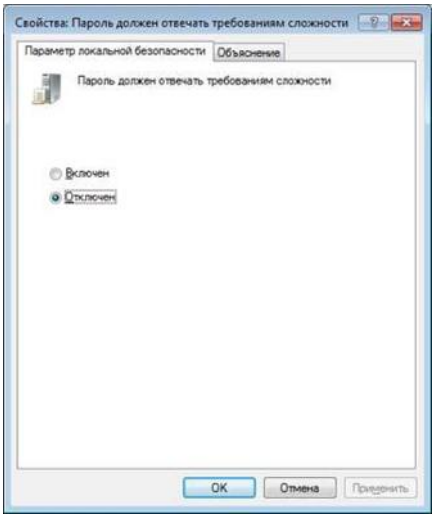


Редактирование групповой политики.

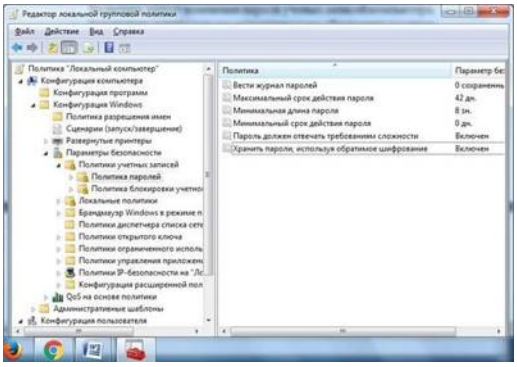
- Минимальную длину пароля установить не менее 8 знаков;



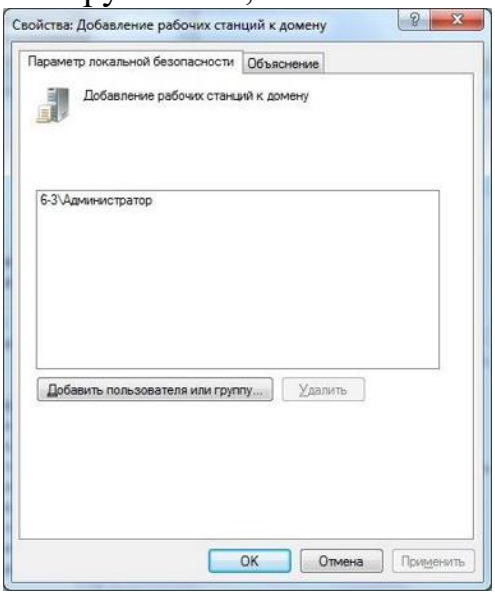
- Включить параметр безопасности, определяющий требования сложности для паролей;



- Включить параметр «Хранить пароли, используя обратимое шифрование»;

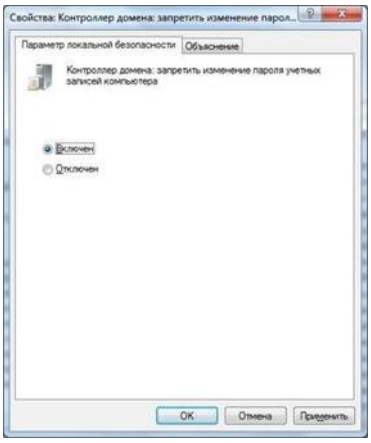


- Разрешить учетной записи «Администратор» добавлять рабочие станции к домену и доступ к компьютеру из сети;

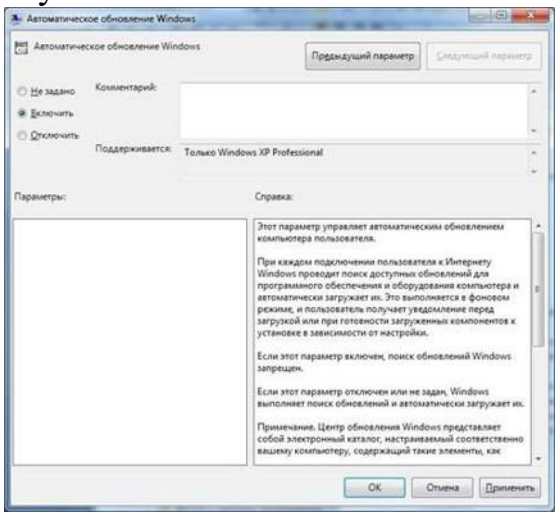


- Разрешить учетной записи «Администратор» изменять системное время;

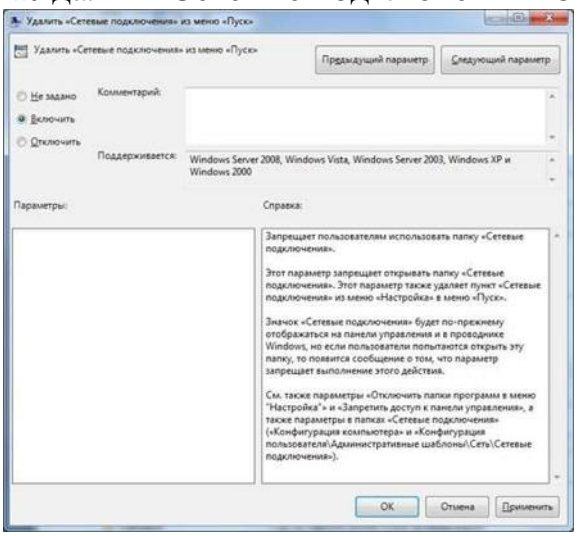
- Включить запрет изменения пароля ученых записей компьютера;



- Установить режим запуска автоматического обновления вручную;



- включить параметр «Удалить Сетевые подключения из меню Пуск»



Контрольные вопросы

1. Для чего предназначены групповые политики?
2. Какие параметры групповых политик являются приоритетными?
3. На какие основные категории делятся параметры политики?
4. На какие компьютеры сети будет распространяться «Групповая политика»?
5. Какие параметры можно изменить при редактировании групповой политики?

Оценивание практических работ:
5(отлично) – работа выполнена полностью, все действия выполнены верно.
4 (хорошо) – работа выполнена не полностью, верно решено 80% задания.
3 (удовлетворительно) – работа выполнена не полностью, верно решено 70% задания.
2 (неудовлетворительно) – работа выполнена не полностью, верно решено менее 60% задания.

3.3 Фонд оценочных средств для рубежного контроля

Рубежный контроль проводится во время аудиторных занятий по ПМ Организация сетевого администрирования в соответствии с учебным планом и рабочей программы ПМ.02 Организация сетевого администрирования.

Вопросы:

1. Оценка и определение параметров развертывания клиентских ОС
2. Планирование стратегии управления образами
3. Реализация безопасности клиентских систем
4. Захват и управление образами клиентских ОС
5. Планирование и реализация миграции пользовательской среды
6. Планирование и развертывание клиентских ОС с помощью Microsoft Deployment Toolkit
7. Планирование и развертывание клиентских ОС с помощью System Center Configuration Manager 2012
8. Планирование и реализация служб удаленного доступа (Remote Desktop Services)
9. Управление виртуализацией пользовательского состояния для клиентских ОС организации
10. Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организации
11. Защита компьютеров предприятия от вредоносных программ и потерь данных
12. Мониторинг производительности и работоспособности инфраструктуры клиентских ОС
13. Разработка стратегии развертывания приложений
14. Диагностика и обеспечение совместимости приложений
15. Развертывание приложений с помощью групповых политик и Windows Intune
16. Развертывание приложений с помощью System Center Configuration Manager
17. Развертывания самообслуживаемых приложений
18. Проектирование и реализация инфраструктуры виртуализации представлений

19. Подготовка, настройка и развертывание представлений виртуализации приложений

20. Проектирование и развертывание среды виртуализации приложений

21. Подготовка к виртуализации и развертывание виртуальных приложений

22. Планирование и реализация безопасности и обновления приложений

23. Планирование и реализация обновления и замены приложений

24. Мониторинг развертывания, использования и производительности приложений

Критерии оценки ответа:

Оценка «отлично» выставляется, если студент:

- полностью раскрыл содержание материала в объеме, предусмотренном программой и учебником, правильно решил задачу;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил чертежи и графики, сопутствующие ответу;
- показал умение иллюстрировать теоретические положения конкретными примерами,

применять их в новой ситуации при выполнении практического задания;

- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя.

Возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя.

Оценка «хорошо» выставляется, если:

ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

Оценка «удовлетворительно» выставляется, если:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения,

достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, чертежах и выкладках, исправленные после нескольких наводящих вопросов преподавателя;

- студент не справился с применением теории в новой ситуации при решении задачи, но выполнил задания обязательного уровня сложности по данной теме;

- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Оценка «неудовлетворительно» выставляется, если:

- не раскрыто основное содержание учебного материала;

- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;

- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя;

- студент обнаружил полное незнание и непонимание изучаемого учебного материала или не смог ответить ни на один из поставленных вопросов по изучаемому материалу.

3.4 Фонд оценочных средств для промежуточной аттестации (экзамен)

На выполнение экзаменационной работы по ПМ дается 18 академических часов/ на диф.зачет по МДК выделяется 2 часа входящих в общее количество часов рабочей программы.

Экзамен по модулю предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.02. Организация сетевого администрирования по специальности СПО 09.02.06. Сетевое и системное администрирование.

Экзамен квалификационный представляет собой ответы на два теоретические вопроса и выполнение практического задания.

Теоретические вопросы:

МДК.02.01. Администрирование сетевых операционных систем

1. Развертывание и управление Windows Server 2012 R2
2. Доменные сервисы Службы Каталога
3. Управление объектами доменных служб Службы Каталога
4. Автоматизация администрирования доменных служб Службы Каталога
5. Применение протокола DHCP
6. Применение DNS
7. Применение локального хранилища данных
8. Применение файловой службы и службы печати

9. Применение групповой политики
10. Защита серверов Windows применением объектов групповой политики
11. Применение серверной виртуализации с Hyper-V
12. Настройка и устранение неполадок службы DNS
13. Поддержка доменных служб Службы Каталога
14. Управление пользовательскими и служебными учетными записями
15. Внедрение инфраструктуры Групповых политик
16. Управление пользовательским рабочим столом через Групповую политику
17. Установка, настройка и устранение неполадок роли Сервер Сетевой политики.
18. Применение защиты доступа к сети
19. Использование удаленного доступа
20. Оптимизация файловых сервисов
21. Настройка шифрования и расширенного аудита
22. Развертывание и поддержка серверных образов
23. Внедрение управления обновлениями
24. Мониторинг Windows Server 2012
25. VMWare vSphere
26. Файловые системы ОС Linux
27. Подготовка сервера ОС Linux
28. Настройка web-серверов в ОС Linux
29. Настройка сервера DNS в ОС Linux
30. Настройка сервера DHCP в ОС Linux
31. Настройка файловых серверов в ОС Linux
32. Настройка серверов БД в ОС Linux
33. Контейнеры Docker
34. Проектирование

МДК.02.02. Программное обеспечение компьютерных сетей

1. Оценка и определение параметров развертывания клиентских ОС
2. Планирование стратегии управления образами
3. Реализация безопасности клиентских систем
4. Захват и управление образами клиентских ОС
5. Планирование и реализация миграции пользовательской среды
6. Планирование и развертывание клиентских ОС с помощью Microsoft Deployment Toolkit
7. Планирование и развертывание клиентских ОС с помощью System Center Configuration Manager 2012
8. Планирование и реализация служб удаленного доступа (Remote Desktop Services)
9. Управление виртуализацией пользовательского состояния для клиентских ОС организации
10. Планирование и реализация инфраструктуры обновлений для поддержки клиентских ОС организации

11. Защита компьютеров предприятия от вредоносных программ и потерь данных
12. Мониторинг производительности и работоспособности инфраструктуры клиентских ОС
13. Разработка стратегии развертывания приложений
14. Диагностика и обеспечение совместимости приложений
15. Развертывание приложений с помощью групповых политик и Windows Intune
16. Развертывание приложений с помощью System Center Configuration Manager
17. Развертывания самообслуживаемых приложений
18. Проектирование и реализация инфраструктуры виртуализации представлений
19. Подготовка, настройка и развертывание представлений виртуализации приложений
20. Проектирование и развертывание среды виртуализации приложений
21. Подготовка к виртуализации и развертывание виртуальных приложений
22. Планирование и реализация безопасности и обновления приложений
23. Планирование и реализация обновления и замены приложений
24. Мониторинг развертывания, использования и производительности приложений

Из данных вопросов формируется 30 билетов, время подготовки студентов 45 минут.

Критерии оценки экзамена

5 «отлично» выставляется, если студент:

- полностью раскрыл содержание материала в объеме, предусмотренном программой и учебником, правильно решил практическое задание;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил практическое задание, сопутствующие ответу;
- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя (возможны одна-две неточности при освещении второстепенных вопросов

или в выкладках, которые студент легко исправил по замечанию преподавателя).

4 «хорошо» выставляется, если:

ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

3 «удовлетворительно» выставляется, если:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, практике и выкладках, исправленные после нескольких наводящих вопросов преподавателя;
- студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме;
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

2 «неудовлетворительно» выставляется, если:

- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;
- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя;
- студент обнаружил полное незнание и непонимание изучаемого учебного материала или не смог ответить ни на один из поставленных вопросов по изучаемому материалу.

Процент результативности	Качественная оценка индивидуальных образовательных достижений	
	балл (отметка)	вербальный аналог
90-100	5	отлично
80-89	4	хорошо
70-79	3	удовлетворительно

менее 70	2	не удовлетворительно

4.Список литературы

Основные источники:

1. Баранчиков А.И., Баранчиков П.А., Громов А.Ю. Организация сетевого администрирования 2017 ОИЦ «Академия»

Интернет ресурсы:

1. Гарант. Информационно-правовой портал [Электронный ресурс] : сайт. – Режим доступа: http://www.garant.ru.
2. Электронно-библиотечная система BOOK.ru [Электронный ресурс]: сайт. – Режим доступа: http://www.book.ru.
3. Российская государственная библиотека [Электронный ресурс] / Центр информ. Технологий РГБ ; ред. Власенко Т.В. ; Web-мастер Козлова Н.В. – Электрон.дан. – М. : Рос.гос. б-ка. – Режим доступа: http://www.rsl.ru.

Приложение 3

РАБОЧАЯ ПРОГРАММА ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ03.Эксплуатация объектов сетевой инфраструктуры

Специальность: 09.02.06 Сетевое и системное администрирование

2020

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

ПМ03.Эксплуатация объектов сетевой инфраструктуры

1.1. Область применения программы профессионального модуля

Рабочая программа профессионального модуля является частью программы подготовки специалистов среднего звена в соответствии с ФГОС СПО по специальности: 09.02.06 Сетевое и системное администрирование в части освоения основного вида профессиональной деятельности: ПМ03.Эксплуатация объектов сетевой инфраструктуры и соответствующих компетенций:

общие компетенции:

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	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.

профессиональные компетенции:

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.

1.2. Цели и задачи профессионального модуля – требования к результатам освоения профессионального модуля:

С целью овладения указанным видом профессиональной деятельности и соответствующими профессиональными компетенциями обучающийся 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

знать:

- архитектуру и функции систем управления сетями, стандарты систем управления;
- средства мониторинга и анализа локальных сетей;
- методы устранения неисправностей в технических средствах

1.3. Количество часов на освоение программы профессионального модуля:

Общая нагрузка – 464 ч., в том числе:
самостоятельная работа – 36 ч.;
теоретические занятия– 80 ч.;
практические занятия – 98 ч.;
консультации – 4 ч.;
промежуточная аттестация – 30 ч.;
учебная практика – 108 ч.;
производственная практика – 108 ч;
Квалификационный экзамен – 18 ч.

2.РЕЗУЛЬТАТЫ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности Эксплуатация объектов сетевой инфраструктуры, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03.	Планировать и реализовывать собственное профессиональное и личностное развитие.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 06.	Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.
ОК 07.	Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.
ОК 08.	Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.
ОК 09.	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.

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.

3. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Структура профессионального модуля

Коды профессиональных, общих компетенций	Наименования разделов профессионального модуля	Общая	Учебная нагрузка							Практики	
			Самостоятельная работа	во взаимодействии с преподавателями						Учебная	Производственная
				Всего по МДК	в том числе						
					Теоретическое обучение	Лаб. Практ.	Курсов. работа	Консультации	Промежуточная аттестация		
1	2	3	4	5	6	7	8	9	10	11	12
ОК 01- ОК 11 ПК 3.1-3.6	Раздел 1. Эксплуатация объектов сетевой инфраструктуры	***130***	***20***	***110***	***48***	***54***		***2***	***6***		
ОК 01- ОК 11 ПК 3.1-3.6	Раздел 2. Безопасность компьютерных сетей	***100***	***16***	***84***	***32***	***44***	***0***	***2***	***6***		
ОК 01- ОК 11 ПК 3.1-3.6	Учебная практика	***108***								***108***	
ОК 01- ОК 11 ПК 3.1-3.6	Производственная практика	***108***									***108***
	Квалификационный экзамен	***18***		***18***					***18***		
	Всего	***464***	***36***		***80***	***98***	***0***	***4***	***30***	***108***	***108***

2.2. Тематический план и содержание профессионального модуля ПМ 03.Эксплуатация объектов сетевой инфраструктуры

Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК)		Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа, курсовая работа	Объем часов	Коды компетенций
1		**2**	**3**	**4**
Раздел ПМ 03. Раздел 1. Эксплуатация объектов сетевой инфраструктуры				
МДК 03.01. Эксплуатация объектов сетевой инфраструктуры			***130/54(20)***	
		8 семестр		
Тема 1.1. Эксплуатация технических средств сетевой инфраструктуры		**Содержание**		
	1	Физические аспекты эксплуатации средств сетевой инфраструктуры.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	2	Физическое вмешательство в инфраструктуру сети.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	3	Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	4	Активное и пассивное сетевое оборудование: кабельные каналы, кабель, патч-панели, розетки.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	5	Полоса пропускания, паразитная нагрузка.	*2*	ОК 01-ОК 11 ПК 3.1-

				3.6
	6	Расширяемость сети. Масштабируемость сети. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	7	Наращивание длины сегментов сети; замена существующей аппаратуры.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	8	Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	9	Техническая и проектная документация. Паспорт технических устройств.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	10	Физическая карта всей сети; логическая топология компьютерной сети.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	11	Классификация регламентов технических осмотров, технические осмотры объектов сетевой инфраструктуры.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	12	Проверка объектов сетевой инфраструктуры и профилактические работы	*2*	ОК 01-ОК 11 ПК 3.1-

				3.6
	13	Проведение регулярного резервирования. Обслуживание физических компонентов; контроль состояния аппаратного обеспечения; организация удаленного оповещения о неполадках.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	14	Программное обеспечение мониторинга компьютерных сетей и сетевых устройств.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	15	Протокол SNMP, его характеристики, формат сообщений, набор услуг.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	16	Задачи управления: анализ производительности и надежности сети.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	17	Оборудование для диагностики и сертификации кабельных систем. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
		Практические занятия		
	18	ПЗ1. Оконцовка кабеля витая пара	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	19	ПЗ 2. Заделка кабеля витая пара в розетку	*2*	ОК 01-ОК 11

				ПК 3.1-3.6
	20	ПЗ. Кроссирование и монтаж патч-панели в коммутационный шкаф, на стену. Тестирование кабеля	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	21	ПЗ 4. Эксплуатация технических средств сетевой инфраструктуры (принтеры, компьютеры, серверы)	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	22	ПЗ5. Выполнение действий по устранению неисправностей	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	23	ПЗ6. Выполнение мониторинга и анализа работы локальной сети с помощью программных средств.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	24	ПЗ7. Оформление технической документации, правила оформления документов	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	25	ПЗ8. Протокол управления SNMP. Основные характеристики протокола SNMP	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	26	ПЗ9. Набор услуг (PDU) протокола SNMP.Формат сообщений SNMP	*2*	ОК 01-ОК 11

				ПК 3.1-3.6
	27	ПЗ10. Задачи управления: анализ производительности сети	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	28	ПЗ11. Задачи управления: анализ надежности сети	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	29	ПЗ12. Управление безопасностью в сети. Учет трафика в сети. Средства мониторинга компьютерных сетей	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	30	ПЗ13. Средства анализа сети с помощью команд сетевой операционной системы	*2*	ОК 01-ОК 11 ПК 3.1-3.6
		Лабораторные работы *не предусмотрены*		
Тема 1.2. Эксплуатация систем IP-телефонии		**Содержание**		
	31	Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper. Многопользовательские конференции. Обеспечение отказоустойчивости.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	32	Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP. Модель установления соединения. Планирование отказоустойчивости.	*2*	ОК 01-ОК 11 ПК 3.1-3.6

	33	Установка и инсталляция программного коммутатора. Монтажные процедуры. Процедуры инсталляции. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов. Внутристанционная маршрутизация.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	34	Управление программным коммутатором. Маршрутизация. Группы соединительных линий. Подключение станций с TDM (абонентский доступ TDM).	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	35	Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP -абоненты. Группы абонентов. Дополнительные абонентские услуги.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	36	Организация эксплуатации систем IP-телефонии. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	37	Восстановление работы сети после аварии. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных;	*2*	ОК 01-ОК 11 ПК 3.1-3.6
		Практические занятия		
	38	ПЗ14. Настройка аппаратных IP-телефонов	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	39	ПЗ15. Настройка программных IP-телефонов, факсов	*2*	ОК 01-ОК 11 ПК 3.1-3.6

	40	ПЗ16. Развертывание сети с использованием VLAN для IP-телефонии	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	41	ПЗ17. Настройка шлюза	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	42	ПЗ18. Установка, подключение и первоначальные настройки голосового маршрутизатора	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	43	ПЗ19. Настройка таблицы пользователей в голосовом маршрутизаторе. Настройка групп в голосовом маршрутизаторе	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	44	ПЗ20. Настройка таблицы маршрутизации вызовов в голосовом маршрутизаторе	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	45	ПЗ21. Настройка голосовых сообщений в маршрутизаторе	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	46	ПЗ22. Настройка программно-аппаратной IP-АТС. Установка и настройка программной IP-АТС (например, Asterisk)	*2*	ОК 01-ОК 11 ПК 3.1-3.6

	47	ПЗ23. Тестирование кодеков. Исследование параметров качества обслуживания	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	48	ПЗ24. Мониторинг и анализ соединений по различным протоколам	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	49	ПЗ25. Мониторинг вызовов в программном коммутаторе	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	50	ПЗ26. Создание резервных копий баз данных	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	51	ПЗ27. Диагностика и устранение неисправностей в системах IP-телефонии	*2*	ОК 01-ОК 11 ПК 3.1-3.6
		Лабораторные работы *не предусмотрены*		
		Самостоятельная работа при изучении раздела МДК03.01.	***20***	
		Примерная тематика внеаудиторной самостоятельной работы		
	1	Физическая инфраструктура сети. Логическая инфраструктура сети	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	2	Сетевые подключения. Протоколы сети.Адресация сети. Система имен сети	*2*	
	3	Автоматическое назначение частных IP-адресов	*2*	
	4	Маршрутизация и инфраструктура сети Windows Server 2012	*2*	
	5	Сетевые компонены Windows	*2*	
	6	Установка сетевых компонентов Windows	*2*	

	7	Установка Active Directory в сети Windows	*2*	
	8	Разбиение на подсети	*2*	
	9	Механизм разбиения на подсети	*2*	
	10	Определение емкости подсети	*2*	
		Консультация	*2*	
Промежуточная аттестация по МДК03.01 в форме		**Экзамена**	*6*	
МДК.03.02. Безопасность компьютерных сетей			***100/44(16)***	
8 семестр				
		Содержание		
	1	Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	2	Безопасность Сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
Тема 2.1. Безопасность компьютерных сетей	3	Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	4	Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	5	Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах.	*2*	ОК 01-ОК 11 ПК 3.1-3.6

	6	Реализация технологий предотвращения вторжения IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	7	Безопасность локальной сети Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2).	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	8	Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	9	Криптографические системы Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	10	Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	11	Реализация технологий VPN VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	12	Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN	*2*	ОК 01-ОК 11 ПК 3.1-3.6

	13	Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	14	Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	15	Cisco ASA Введение в Адаптивное устройство безопасности ASA. Конфигурация файервола на базе ASA с использованием графического интерфейса ASDM.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	16	Cisco ASA Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.	*2*	ОК 01-ОК 11 ПК 3.1-3.6
		Практические занятия		
	17	ПЗ1.Социальная инженерия	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	18	ПЗ2.Исследование сетевых атак и инструментов проверки защиты сети	*2*	
	19	ПЗ3.Настройка безопасного доступа к маршрутизатору	*2*	
	20	ПЗ4.Обеспечение административного доступа AAA и сервера Radius	*2*	
	21	ПЗ5.Настройка политики безопасности брандмауэров	*2*	
	22	ПЗ6.Настройка системы предотвращения вторжений (IPS)	*2*	
	23	ПЗ7.Настройка безопасности на втором уровне на коммутаторах	*2*	
	24	ПЗ8.Исследование методов шифрования	*2*	
	25	ПЗ9.Настройка Site-to-SiteVPN используя интерфейс командной строки	*2*	
	26	ПЗ10.Базовая настройка шлюза безопасности ASA используя интерфейс командной строки	*2*	
	27	ПЗ11.Настройка брандмауэров используя интерфейс командной строки	*2*	
	27	ПЗ12.Базовая настройка шлюза безопасности ASA используя ASDM	*2*	
	29	ПЗ13.Настройка брандмауэров используя ASDM	*2*	
	30	ПЗ14.Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	*2*	

	31	П315. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	32	П316. НастройкаClientless Remote Access SSL VPNs используя ASDM	*2*	
	33	П317. НастройкаClientless Remote Access SSL VPNs используя ASDM	*2*	
	34	П318. Настройка AnyConnect Remote Access SSL VPN используя ASDM	*2*	
	35	П319.Настройка AnyConnect Remote Access SSL VPN используя ASDM	*2*	
	36	П320. Комплексная лабораторная работа по безопасности	*2*	
	37	П321. Комплексная лабораторная работа по безопасности	*2*	
	38	П322. Комплексная лабораторная работа по безопасности	*2*	
		Лабораторные работы *не предусмотрены*		
		Самостоятельная работа при изучении раздела МДК03.02.	***16***	
		Примерная тематика внеаудиторной самостоятельной работы		
	1	Поиск неисправностей по принципу локализации неисправностей конкретного оборудования	*2*	ОК 01-ОК 11 ПК 3.1-3.6
	2	Изучение принципа работы новых контрольно-измерительных аппаратов	*2*	
	3	Основные сведения о политиках удаленного доступа Устранение неполадок при подключениях удаленного доступа	*2*	
	4	Реализация процедур безопасного администрирования сети	*2*	
	5	Оснастка Шаблоны безопасности	*2*	
	6	Схемы обжимки витой пары	*2*	
	7	Устройство «пакета», передаваемого по сети	*2*	
	8	Использование бесклассовой междоменной маршрутизации. Маски подсети переменной длины	*2*	
		Консультация	*2*	
Промежуточная аттестация по МДК03.02 в форме		**Экзамена**	*6*	
Учебная практика			***108***	
Виды работ	1	Ознакомление с программой практики. Техника безопасности. Правила поведения.	*6*	ОК 01-ОК 11 ПК 3.1-3.6
	2	Настройка прав доступа.	*6*	
	3	Оформление технической документации, правила оформления документов.	*6*	
	4	Настройка аппаратного и программного обеспечения сети.	*6*	
	5	Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	*6*	
	6	Программная диагностика неисправностей.	*6*	
	7	Аппаратная диагностика неисправностей.	*6*	
	8	Поиск неисправностей технических средств.	*6*	
	9	Выполнение действий по устранению неисправностей.	*6*	

	10	Использование активного, пассивного оборудования сети.	*6*	ОК 01-ОК 11 ПК 3.1-3.6
	11	Устранение паразитирующей нагрузки в сети.	*6*	
	12	Построение физической карты локальной сети.	*6*	
	13	Настройка прав доступа.	*6*	
	14	Оформление технической документации, правила оформления документов.	*6*	
	15	Настройка аппаратного и программного обеспечения сети.	*6*	
	16	Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	*6*	
	17	Программная диагностика неисправностей.	*6*	
	18	Написание и оформление отчета по практике	*6*	
Производственная практика Виды работ			***108***	
	1	Ознакомление с программой практики. Техника безопасности. Правила поведения.		
	2	Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.	*6*	ОК 01-ОК 11 ПК 3.1-3.6
	3	Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.	*6*	
	4	Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.	*6*	
	5	Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.	*6*	
	6	Установка прав доступа и контроль использования сетевых ресурсов.	*6*	
	7	Установка прав доступа и контроль использования сетевых ресурсов.	*6*	
	8	Обеспечение своевременного копирования, архивирования и резервирования данных.	*6*	
	9	Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.	*6*	
	10	Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.	*6*	
	11	Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.	*6*	
	12	Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.	*6*	
	13	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.	*6*	
	14	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.	*6*	

	15	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	*6*	ОК 01-ОК 11 ПК 3.1-3.6
	16	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	*6*	
	17	Документирование всех произведенных действий.	*6*	
	18	Написание и оформление отчета по практике	*6*	
		Квалификационный экзамен	***18***	
		Всего:	***464/98(36)***	
Промежуточная аттестация по учебной практике в форме дифференцированного зачета				
Промежуточная аттестация по производственной практике в форме дифференцированного зачета				
Промежуточная аттестация по профессиональному модулю: квалификационный экзамен				

4. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

4.1. Требования к минимальному материально-техническому обеспечению

Реализация программы модуля требует наличия следующих специальных помещений:

Лаборатории «Организация и принципы построения компьютерных систем», оснащенные в соответствии с п. 6.1.2.1. Примерной программы по специальности 09.02.06 «Сетевое и системное администрирование»**.**

Для выполнения практических лабораторных занятий курса в группах (до 15 человек) требуются компьютеры и периферийное оборудование в приведенной ниже конфигурации:

– 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;

– Специализированная эргономичная мебель для работы за компьютером;

– Офисный мольберт (флипчарт);

– Проектор и экран;

– Маркерная доска;

– Принтер А3, цветной;

– Программное обеспечение общего и профессионального назначения.

Оснащенные базы практики, в соответствии с Программой подготовки специалистов среднего звена по специальности 09.02.06 «Сетевое и системное администрирование».

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Основные источники:

1. Назаров А.В., Мельников В.П., Куприянов А.И. Эксплуатация объектов сетевой инфраструктуры ОИЦ «Академия». 2017.

Интернет ресурсы:

2. Гарант. Информационно-правовой портал [Электронный ресурс] : сайт. – Режим доступа: http://www.garant.ru.

3. Электронно-библиотечная система BOOK.ru [Электронный ресурс]: сайт. – Режим доступа: http://www.book.ru.

4. Российская государственная библиотека [Электронный ресурс] / Центр информ. Технологий РГБ ; ред. Власенко Т.В. ; Web-мастер Козлова Н.В. – Электрон.дан. – М. : Рос.гос. б-ка. – Режим доступа: http://www.rsl.ru.

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

Код и наименование профессиональных и общих компетенций, формируемых в рамках модуля	Критерии оценки	Методы оценки
ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам
ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам
ПК 3.3. Устанавливать, настраивать, эксплуатировать и обслуживать сетевые конфигурации	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам
ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам

ПК 3.5. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам
ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.	Оценка «**отлично**» - техническое задание проанализировано, алгоритм разработан, соответствует техническому заданию и оформлен в соответствии со стандартами, пояснены его основные структуры. Оценка «**хорошо**» -алгоритм разработан, оформлен в соответствии со стандартами и соответствует заданию, пояснены его основные структуры. Оценка «**удовлетворительно**» - алгоритм разработан и соответствует заданию.	Экзамен, практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и работам

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

09.	информационные технологии в профессиональной деятельности	информационно-коммуникационных технологий в профессиональной деятельности согласно формируемым умениям и получаемому практическому опыту;	
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.	- 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 планировать предпринимательскую деятельность в профессиональной сфере при проведении работ по конструированию сетевой инфраструктуры	

ПМ 03. Эксплуатация объектов сетевой инфраструктуры

Календарный план по учебной практике

№ п/п	Содержание	Кол-во часов/дней	Примечание
1	Ознакомление с программой практики. Техника безопасности. Правила поведения.	**6/1**	
2	Настройка прав доступа.	**6/1**	
3	Оформление технической документации, правила оформления документов.	**6/1**	
4	Настройка аппаратного и программного обеспечения сети.	**6/1**	
5	Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	**6/1**	
6	Программная диагностика неисправностей.	**6/1**	
7	Аппаратная диагностика неисправностей.	**6/1**	
8	Поиск неисправностей технических средств.	**6/1**	
9	Выполнение действий по устранению неисправностей.	**6/1**	
10	Использование активного, пассивного оборудования сети.	**6/1**	
11	Устранение паразитирующей нагрузки в сети.	**6/1**	
12	Построение физической карты локальной сети.	**6/1**	
13	Настройка прав доступа.	**6/1**	
14	Оформление технической документации, правила оформления документов.	**6/1**	
15	Настройка аппаратного и программного обеспечения сети.	**6/1**	
16	Настройка сетевой карты, имя компьютера, рабочая группа, введение компьютера в domain.	**6/1**	
17	Программная диагностика неисправностей.	**6/1**	
18	Написание и оформление отчета по практике	**6/1**	
	ИТОГО	**108/36**	

Календарный план по производственной практике (по профилю специальности)

№ п/п	Содержание	Кол-во часов/дней	Примечание
1	Ознакомление с программой практики. Техника безопасности. Правила поведения.	**6/1**	
2	Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение.	**6/1**	
3	Осуществление конфигурирования программного обеспечения на серверах и рабочих станциях.	**6/1**	
4	Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций.	**6/1**	
5	Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли.	**6/1**	
6	Установка прав доступа и контроль использования сетевых ресурсов.	**6/1**	
7	Установка прав доступа и контроль использования сетевых ресурсов.	**6/1**	
8	Обеспечение своевременного копирования, архивирования и резервирования данных.	**6/1**	
9	Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.	**6/1**	
10	Принятие мер по восстановлению работоспособности локальной сети при сбоях или выходе из строя сетевого оборудования.	**6/1**	
11	Выявление ошибок пользователей и программного обеспечения и принятие мер по их исправлению.	**6/1**	
12	Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети.	**6/1**	
13	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.	**6/1**	
14	Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия.	**6/1**	
15	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	**6/1**	
16	Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций.	**6/1**	
17	Документирование всех произведенных действий.	**6/1**	
18	Написание и оформление отчета по практике	**6/1**	
	ИТОГО	**108/36**	

Вид промежуточной аттестации: дифференцированный зачёт

Приложение 3А

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по ПМ
ПМ.03 Эксплуатация объектов сетевой инфраструктуры

Специальность: 09.02.06 Сетевое и системное администрирование

СОДЕРЖАНИЕ

1.Пояснительная записка

Фонд оценочных средств по профессиональному модулю Эксплуатация объектов сетевой инфраструктуры разработан на основании требований ФГОС СПО, с учетом профессиональной направленности программ среднего профессионального образования.

Основная цель создания фонда оценочных средств профессионального модуля – совершенствование содержания профессионального модуля для формирования профессионально - значимых компетенций. Фонд оценочных средств представлен комплектом контрольно-оценочных средств.

ФОС состоит из оценочных средств для: текущего контроля, рубежного контроля и промежуточной аттестации обучающихся.

2.Описание контрольно-оценочных средств

Фонд оценочных средств для текущего, рубежного контроля и промежуточной аттестации разработан для оценки уровня освоения обучающимися планируемых результатов. В ФОС раскрыта типология оценочных ситуаций и заданий текущего, рубежного контроля и промежуточной аттестации, по итогам освоения разделов основного содержания профессионального модуля.

Структурные элементы ФОС по профессиональному модулю:

- результаты освоения ПМ, подлежащие проверке;
- описание контрольно-оценочных средств;
- разноформатные задания для текущего контроля по ПМ;
- разноформатные задания для рубежного контроля по ПМ;
- разноформатные задания для промежуточной аттестации по ПМ.

Кроме оценочных заданий, ФОС включает эталоны ответов к некоторым заданиям, а к типовым – алгоритмы решения либо ориентировочную основу действий.

2.1 Планируемые результаты освоения ПМ 03. Эксплуатация объектов сетевой инфраструктуры

Планируемые результаты освоения профессионального модуля в соответствии с ФГОС СПО

Таблица 1

Код ПК, ОК	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств; осуществлять диагностику и поиск неисправностей	архитектуру и функции систем управления сетями, стандарты систем управления; средства мониторинга и анализа локальных
ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.		
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.		
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.		

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.	всех компонентов сети; выполнять действия по устранению неисправностей	сетей; методы устранения неисправностей в технических средствах
ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.		
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности		
ОК 09. 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.		
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.		

3.Фонды оценочных средств

3.1 Фонд оценочных средств для текущего контроля

Текущий контроль проводится во время аудиторных занятий по ПМ

Эксплуатация объектов сетевой инфраструктуры в соответствии с учебным планом и рабочей программы ПМ 03. Эксплуатация объектов сетевой инфраструктуры.

ТЕМА 1. ФУНДАМЕНТАЛЬНЫЕ ПРИНЦИПЫ БЕЗОПАСНОЙ СЕТИ

УСТНЫЙ ОПРОС ПО ТЕМЕ «ФУНДАМЕНТАЛЬНЫЕ ПРИНЦИПЫ БЕЗОПАСНОЙ СЕТИ»

Вопросы:

1. Современные угрозы сетевой безопасности.
2. Вирусы, черви и троянские кони.
3. Методы атак.

Критерии оценки устного ответа

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ»

Задача

В этой практической работе вы изучите примеры социальной инженерии, определите пути ее определения и противодействия ей.

Ресурсы

Компьютер с доступом в Интернет

Примеры социальной инженерии

Термин «социальная инженерия» в сфере информационной безопасности используется для описания техник, применяемых человеком (или группой людей) для манипулирования другими людьми с целью получения доступа или компрометации информации об организации или ее информационных системах. Злоумышленника, который использует эту технологию, обычно трудно определить, он может называть себя новым сотрудником, сотрудником обслуживающего персонала или исследователем. Социальный инженер может даже предоставлять документы, подтверждающие его личность. Втираясь в доверие и задавая вопросы, он или она могут собрать достаточно информации для внедрения в информационную сеть организации.

С помощью любого браузера найдите информацию о случаях применения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.

_____

_____

Определение признаков социальной инженерии

Социальные инженеры – не что иное, как воры или шпионы. Вместо того чтобы получить доступ к вашей сети через Интернет, они пытаются получить его, используя желание человека быть любезным. И хотя пример ниже не относится к сетевой безопасности, он показывает, каким образом ничего не подозревающий человек может невольно разгласить конфиденциальную информацию.

«Это кафе было достаточно тихим, и я, одетый в костюм, сел за свободный столик. Я поставил портфель на стол и ждал подходящую жертву. Вскоре подобная жертва появилась – вместе с подругой они расположились за соседним столиком. Она положила сумочку на соседний стул, пододвинула его поближе и все время держала руку на сумочке.

Через несколько минут ее подруга вышла в уборную. Жертва [цель] осталась одна, и я подал Алексу и Джесс сигнал. Играя роль парочки, Алекс и Джесс спросили у жертвы, сможет ли она их сфотографировать вместе. Она с радостью согласилась. Она убрала руку с сумочки, взяла камеру и сфотографировала «счастливую парочку». В это время я, пользуясь ее невнимательностью, нагнулся, взял ее сумочку, положил в портфель и закрыл его. Жертва даже не замечала пропажи в то время, как Алекс и Джесс уходили из кафе. После этого Алекс пошел на парковку неподалеку.

Прошло немного времени, прежде чем она поняла, что ее сумочка пропала. Она начала паниковать, повсюду суетливо искать сумочку. Это было именно то, на что я надеялся. Я спросил, не нужна ли ей моя помощь.

Она спросила, не видел ли я что-то. Я сказал, что не видел, но убедил присесть и подумать о том, что было в той сумочке. Телефон. Косметика. Немного наличных. Кредитные карты. Бинго!

Я спросил, в каком банке она обслуживалась, а затем объявил, что работаю на этот банк. Какая удача! Я убедил ее в том, что все будет хорошо, но ей нужно прямо сейчас заблокировать свою кредитную карту. Я позвонил по номеру «техподдержки», по которому на самом деле ответил Алекс, и передал ей свой телефон.

Алекс находился в фургоне на парковке. Магнитола на приборной панели воспроизводила шум офиса. Он уверил жертву, что ее карту можно с легкостью заблокировать, но для того, чтобы подтвердить ее личность, требуется ввести PIN-код на клавиатуре телефона, с которого она звонит. На клавиатуре моего телефона.

Когда мы получили ее ПИН-код, я ушел. Если бы мы были реальными ворами, мы бы могли получить доступ к ее счету при помощи банкомата или

покупок с подтверждением PIN-кодом. К счастью для нее, это было всего лишь ТВ-шоу».

«Взлом или социальная инженерия – автор Christopher Hadnagy http://www.hackersgarage.com/
hacking-vs-social-engineering.html

На заметку: «Те, кто возводят стены, думают иначе, чем те, кто пытаются преодолеть эту стену снизу, сверху, вокруг или сквозь нее». Paul Wilson – The Real Hustle.

Найдите способы определения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.

_____

_____

Анализ способов предотвращения применения социальной инженерии

Приняты ли в вашей компании или школе процедуры, призванные предотвращать применение социальной инженерии?

_____

Если да, в чем заключаются эти процедуры?

_____

_____

Найдите в Интернете процедуры, принятые в организациях для того, чтобы предотвратить получение доступа к конфиденциальной информации при помощи социальной инженерии. Перечислите найденное.

_____

_____

Критерии оценивания практической работы

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА
ИССЛЕДОВАНИЕ СЕТЕВЫХ АТАК И ИНСТРУМЕНТОВ ПРОВЕРКИ ЗАЩИТЫ СЕТИ

Задачи

Часть 1. Изучение сетевых атак

Изучите произошедшие сетевые атаки.

Выберите сетевую атаку и составьте по ней отчет для представления его аудитории.

Часть 2. Изучение инструментов аудита безопасности и проведения атак

Изучите инструменты аудита безопасности.

Выберите один из инструментов и составьте его презентацию для класса.

Исходные данные/сценарий

За многие годы злоумышленники разработали множество инструментов для проведения атак и компрометации сетей. Эти атаки имеют множество форм, но чаще всего они направлены на получение конфиденциальной информации, уничтожение ресурсов или блокирование доступа легальных пользователей к ресурсам. Когда сетевые ресурсы оказываются недоступны, может страдать продуктивность работника, приводя к упущенной выгоде для всего бизнеса.

Чтобы понять, как защитить сеть от атак, администратор должен определить уязвимости сети. Специальные программы аудита безопасности, разработанные производителями оборудования и программного обеспечения, помогают определить потенциальные уязвимости. Инструменты, которые применяются для атак на сеть, могут быть использованы и сетевыми специалистами для тестирования способности сети противостоять этим атакам. После определения уязвимостей можно предпринимать меры для защиты сети.

Эта лабораторная работа представляет собой структурированный исследовательский проект, разделенный на две части: изучение сетевых атак и инструментов аудита безопасности. Сообщите инструктору, какие сетевые атаки и инструменты для аудита безопасности вы выбрали для изучения. Таким образом, участники группы расскажут о целом наборе сетевых атак и инструментов для определения уязвимостей.

В части 1 изучите реально произошедшие сетевые атаки. Выберите одну из этих атак и опишите, каким образом она была совершена, объем урона, нанесенного сети, и время простоя. Затем проанализируйте, каким образом данная атака могла бы быть нейтрализована и какие техники нейтрализации можно реализовать для предотвращения будущих атак. В конце подготовьте отчет по форме, описанной в этой лабораторной работе.

В части 2 изучите инструменты аудита безопасности и проведения атак. Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Составьте отчет на одну страницу по этому инструменту по форме, описанной в этой лабораторной работе. Подготовьте короткую (на 5-10 минут) презентацию для группы.

Вы можете работать в парах, где один человек рассказывает о сетевой атаке, а другой – об инструментах. Каждый участник группы составляет короткий рассказ о результатах своего анализа. Можно использовать презентации Powerpoint или просто продемонстрировать полученные результаты.

Необходимые ресурсы

Компьютер с доступом в Интернет

Компьютер для проведения презентаций с установленным Powerpoint или другим программным обеспечением для презентаций

Видеопроектор и экран для демонстраций и презентаций

Изучение сетевых атак

В части 1 данной практической работы вы изучите реальные сетевые атаки и выберете одну из них для составления отчета. Заполните форму ниже на основе результатов своего анализа.

Изучите различные сетевые атаки.

Перечислите несколько атак, которые вы обнаружили в ходе изучения.

_____

Заполните следующую форму по выбранной сетевой атаке.

Название атаки	
Тип атаки	
Даты проведения атак	
Пострадавшие компьютеры/организации	
Принцип действия и результаты	
Варианты нейтрализации	
Справочные данные и ссылки	
Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)	

Изучение инструментов аудита безопасности и проведения атак

Во второй части данной практической работы изучите инструменты для аудита безопасности и проведения атак. Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Заполните форму ниже на основе полученных результатов.

Изучите различные инструменты аудита безопасности и проведения атак.

Перечислите несколько инструментов, которые вы обнаружили в ходе изучения.

_____

Заполните следующую форму для выбранного инструмента аудита безопасности/проведения атак.

Наименование инструмента	

Разработчик	
Тип инструмента (с интерфейсом или символьно-ориентированный)	
Место использования (сетевое устройство или компьютер)	
Стоимость	
Описание ключевых особенностей и возможностей продукта или инструмента	
Справочные данные и ссылки	

Критерии оценивания практической работы

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

«БЕЗОПАСНОСТЬ СЕТЕВЫХ УСТРОЙСТВ OSI»

Вопросы:

1. Безопасный доступ к устройствам.
2. Назначение административных ролей.
3. Мониторинг и управление устройствами.
4. Использование функция автоматизированной настройки безопасности.

Критерии оценки устного ответа

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

Тест на тему: Уровни модели OSI

Вариант №1

1. Модель OSI описывает:

А) правила и процедуры передачи данных в различных сетевых средах при организации сеанса связи;

Б) только правила передачи данных в различных сетевых средах при организации сеанса связи;

В) только процедуры передачи данных в различных сетевых средах при организации сеанса связи.

2. На сколько уровней модель OSI разделяет коммуникационные функции:

А) 5;

Б) 8;

В) 7.

3. Какие задачи выполняют уровни OSI в процессе передачи данных по сети:

А) уровни выполняют одинаковые задачи, постоянно повторяя передающие сигналы по сети;

Б) каждый уровень выполняет свою определенную задачу;

В) первых три уровня выполняют одинаковые задачи, последующие выполняют определенные задачи.

4. Выбрать правильное расположение уровней модели OSI от 7 до 1:

А) прикладной, канальный, представительский, сеансовый, транспортный, сетевой, физический;

Б) представительский, прикладной, сеансовый, транспортный, сетевой, канальный, физический;

В) прикладной, представительский, сеансовый, транспортный, сетевой, канальный, физический.

5. Верно ли утверждение: «Каждый уровень модели выполняет свою функции. Чем выше уровень, тем более сложную задачу он решает»:

А) верно;

Б) не верно.

6. На базе протоколов, обеспечивающих механизм взаимодействия программ и процессов на различных машинах, строится:

А) горизонтальная модель;

Б) вертикальная модель;

В) сетевая модель.

7. На основе услуг, обеспечиваемых соседними уровнями друг другу на одной машине строится:

А) горизонтальная модель;

Б) вертикальная модель;

В) сетевая модель.

8. Какой уровень представляет собой набор интерфейсов, позволяющим получить доступ к сетевым службам:

А) представительский;

Б) прикладной;

В) сеансовый.

9. Какой уровень обеспечивает контроль логической связи и контроль доступа к среде:

А) представительский;

Б) прикладной;

В) канальный.

10. Какой уровень преобразует данные в общий формат для передачи по сети:

А) сетевой;

Б) представительский;

В) сеансовый.

Вариант №2

1. Какой уровень обеспечивает битовые протоколы передачи информации:

А) сетевой;

Б) транспортный;

В) физический.

2. Какой уровень управляет передачей данных по сети и обеспечивает подтверждение передачи:

А) транспортный;

Б) канальный;

В) сеансовый.

3. Какой уровень поддерживает взаимодействие между удаленными процессами:

А) транспортный;

Б) канальный;

В) сеансовый.

4. Какой уровень управляет потоками данных, преобразует логические сетевые адреса и имена в соответствующие им физические:

А) сетевой;

Б) представительский;

В) транспортный.

5. Единица данных, которой оперирует прикладной уровень, называется:

А) пакетом;

Б) сообщением;

В) потоком.

6. При какой передаче прикладные процессы будут передавать данные, и принимать их одновременно?

А) дуплексная передача;

Б) полудуплексная передача.

7. При какой передаче прикладные процессы будут передавать и принимать данные по очереди?

А) дуплексная передача;

Б) полудуплексная передача.

8. Единицей информации канального уровня являются:

А) сообщения;

Б) потоки;

В) кадры.

9. Под физической средой понимают:

А) материальную субстанцию, через которую осуществляется передача сигнала;

Б) материальную субстанцию, из которой состоит материнская плата;

В) совокупность сигналов.

10. Основными элементами модели OSI являются:

А) уровни;

Б) уровни и прикладные процессы;

В) уровни, прикладные процессы и физические средства соединения.

Ключи к тесту

Вариант №1		Вариант №2	
1-А	6-А	1-В	6-А
2-В	7-Б	2-А	7-Б
3-Б	8-Б	3-В	8-В
4-В	9-В	4-А	9-А
5-А	10-Б	5-Б	10-В

Критерии оценивания теста

5 (отлично) – правильно выполнены 9-10 заданий.

4 (хорошо) – правильно выполнены 7-8 заданий.

3 (удовлетворительно) – правильно выполнены 5-6 заданий.

2 (неудовлетворительно) – правильно выполнены менее 5 заданий.

«АВТОРИЗАЦИЯ, АУТЕНТИФИКАЦИЯ И УЧЕТ ДОСТУПА»

Вопросы:

1. Свойства AAA.
2. Локальная AAA аутентификация.
3. Server-based AAA.

Критерии оценки устного ответа

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

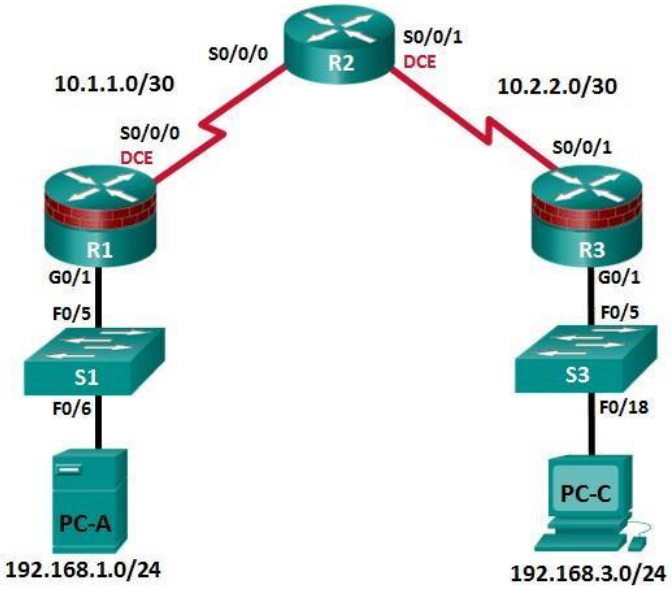
«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА
ОБЕСПЕЧЕНИЕ АДМИНИСТРАТИВНОГО ДОСТУПА AAA И СЕРВЕРА RADIU

Топология



Примечание. В устройствах ISR G1 используются интерфейсы FastEthernet вместо GigabitEthernet.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6

PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

- Настройте основные параметры, такие как имена хостов, IP-адреса интерфейсов и пароли для доступа.
- Настройте статическую маршрутизацию.

Часть 2. Настройка локальной аутентификации

- Настройте локального пользователя базы данных и локальный доступ для линий консоли, vty и aux.
- Проверьте конфигурацию.

Часть 3. Настройка локальной аутентификации с помощью AAA

- Настройте локальную базу данных пользователей с помощью Cisco IOS.
- Настройте локальную аутентификацию AAA с помощью Cisco IOS.
- Проверьте конфигурацию.

Часть 4. Настройка централизованной аутентификации с помощью AAA и RADIUS

- Установите на компьютер сервер RADIUS.
- Настройте пользователей на сервере RADIUS.
- На маршрутизаторе настройте сервисы AAA с помощью Cisco IOS, чтобы получить доступ к серверу RADIUS для аутентификации.
- Проверьте конфигурацию AAA и RADIUS.

Исходные данные/сценарий

Самым распространенным способом обеспечения безопасного доступа к маршрутизатору является создание паролей для линий консоли, vty и aux. При попытке доступа к маршрутизатору у пользователя будет запрашиваться только пароль. Настройка секретного пароля в привилегированном режиме повышает уровень безопасности, но в любом случае для каждого уровня доступа требуется только основной пароль.

Помимо основных паролей, в локальной базе данных маршрутизатора можно настроить отдельные имена или учетные записи пользователей с разными уровнями привилегий, которые могут применяться ко всему маршрутизатору. Когда для линий консоли, vty или aux настроено обращение к этой локальной базе данных, то при использовании любой из этих линий для доступа к маршрутизатору пользователю предлагается ввести имя и пароль.

Для дополнительного контроля над процессом входа может применяться метод аутентификации, авторизации и учета (AAA). Для обеспечения базовой аутентификации функцию AAA можно настроить на доступ к локальной базе данных при вводе имен пользователей. Кроме того, могут быть определены запасные процедуры. Однако данный подход не обладает хорошей масштабируемостью, так как его нужно настраивать на каждом маршрутизаторе. Для обеспечения максимальной масштабируемости и максимально эффективного применения AAA, данную функцию нужно использовать совместно с базой данных внешнего сервера TACACS+ или

RADIUS. При попытке пользователя войти в систему маршрутизатор обращается к внешнему серверу базы данных для проверки действительности имени пользователя и пароля.

В данной лабораторной работе вы построите сеть из нескольких маршрутизаторов и настроите маршрутизаторы и хосты. Затем вам будет необходимо использовать команды CLI для настройки на маршрутизаторах базовой локальной аутентификации с помощью AAA. Вы установите на внешнем компьютере программное обеспечение RADIUS и будете использовать AAA для аутентификации пользователей с помощью сервера RADIUS.

Необходимые ресурсы

- 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2 и лицензией Security Technology Package)
- 2 коммутатора (Cisco 2960 или аналогичный) (необязательно)
- 2 ПК (Windows 7 или 8.1, с установленным SSH-клиентом и WinRadius)
- Последовательные кабели и кабели Ethernet, как показано на топологической схеме
- Консольные кабели для настройки сетевых устройств Cisco

Часть 1: Настройка основных параметров устройства

В части 1 этой лабораторной работы вы создадите топологию сети и настроите основные параметры, такие как IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.

Все операции должны быть выполнены на маршрутизаторах R1 и R3. На маршрутизаторе R2 необходимо выполнить только шаги 1, 2, 3 и 6. В качестве примера здесь показана процедура для маршрутизатора R1.

Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.

Шаг 2: Настройте основные параметры для каждого маршрутизатора.

a. Задайте имена хостов согласно топологической схеме.
b. Настройте IP-адреса, как показано в таблице IP-адресов.
c. Настройте тактовую частоту маршрутизаторов с помощью DCE-кабеля, подключенного к последовательному интерфейсу каждого из них.

R1(config)# **interface S0/0/0**

R1(config-if)# **clock rate 64000**

d. Чтобы маршрутизатор не пытался неправильно интерпретировать введенные команды как имена хостов, отключите функцию DNS-поиска.

R1(config)# **no ip domain-lookup**

Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.

a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из маршрутизатора R3 в R2.

b. Настройте статический маршрут из маршрутизатора R2 к LAN маршрутизатора R1 и статический маршрут из маршрутизатора R2 к LAN маршрутизатора R3.

Шаг 4: Настройте параметры IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показано в таблице IP-адресов.

Шаг 5: Проверьте связь между компьютером PC-A и маршрутизатором R3.

a. Отправьте эхо-запрос с маршрутизатора R1 на маршрутизатор R3. Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.
b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-C в локальной сети маршрутизатора R3.

   Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем, как продолжить.

   Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, то это означает, что статическая маршрутизация настроена верно и работает исправно. Если эхо-запрос был выполнен с ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командами **show run** и **show ip route**, чтобы определить проблемы, связанные с протоколом маршрутизации.

Шаг 6: Сохраните основную текущую конфигурацию для каждого маршрутизатора.

Шаг 7: Сконфигурируйте и зашифруйте пароли на маршрутизаторах R1 и R3.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегчения процесса выполнения лабораторной работы пароли были относительно упрощены. В производственной сети рекомендуется использовать более сложные пароли.

На данном шаге настройте параметры одинаковым образом на маршрутизаторах R1 и R3. В качестве примера здесь показан маршрутизатор R1.

a. Задайте минимальную длину пароля.

   Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

   R1(config)# **security passwords min-length 10**
b. Настройте пароль **enable secret** на обоих маршрутизаторах. Используйте алгоритм хеширования type 9 (SCRYPT).

   R1(config)# **enable algorithm-type scrypt secret cisco12345**

Шаг 8: Настройте основную консоль, вспомогательный порт и линии vty.

a. Настройте пароль консоли и активируйте вход в систему для маршрутизатора 1. Для дополнительной безопасности команда **exec-timeout** обеспечивает выход из системы линии, если в течение **5** минут отсутствует активность. Команда **logging synchronous** предотвращает прерывание ввода команд сообщениями консоли. **Примечание.** Чтобы исключить необходимость постоянного повторного входа в систему во время лабораторной работы, вы можете ввести команду **exec-timeout** с параметрами 0 0, чтобы отключить проверку истечения времени ожидания. Однако такой подход не считается безопасным.

```
R1(config)# line console 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous
```

b. Настройте пароль для порта AUX для маршрутизатора R1.

```
R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

c. Настройте пароль на линиях vty для маршрутизатора R1.

```
R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
```

d. Зашифруйте пароли для консоли, aux и vty.

```
R1(config)# service password-encryption
```

e. Введите команду **show run**. Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

Шаг 9: Настройте предупреждающий баннер при входе в систему на маршрутизаторах R1 и R3.

a. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневным сообщением (MOTD) с помощью команды **banner motd**. При подключении пользователя к маршрутизатору до запроса на ввод авторизационных данных отображается баннер MOTD. В данном примере в начале и конце сообщения используется знак доллара ($).

```
R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit
```

b. Выйдите из привилегированного режима с помощью команды **disable** или **exit**, а затем нажмите **Enter** для начала работы.

Если баннер отображается некорректно, создайте его заново с помощью команды **banner motd.**

Шаг 10: Сохраните базовые конфигурации на всех маршрутизаторах.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

R1# **copy running-config startup-config**

Часть 2: Настройка локальной аутентификации

В части 2 данной лабораторной работы необходимо создать локальное имя пользователя и пароль, а также настроить способ доступа к линиям консоли, aux и vty через локальную базу данных маршрутизатора, где находятся действительные имена пользователей и пароли. Выполните все шаги на маршрутизаторах R1 и R3. Ниже показана процедура для маршрутизатора R1.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования MD5. Используйте алгоритм хеширования type 9 (SCRYPT).

R1(config)# **username user01 algorithm-type scrypt secret user01pass**

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

_____

_____

Шаг 2: Настройте локальную аутентификацию для линии консоли и входа в систему.

a. Настройте линию консоли на использование локально определенных имен пользователей и паролей.

R1(config)# **line console 0**

R1(config-line)# **login local**

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R1 con0 is now available. Press RETURN to get started.

c. Войдите в систему с помощью ранее настроенной учетной записи **user01** и пароля.

Чем сейчас отличается вход через консоль от того, что было раньше?

_____

_____

d. После входа введите команду **show run.** Вам удалось отправить команду? Поясните ответ.

_____

_____

Войдите в привилегированный режим, используя команду **enable**. У вас был запрошен пароль? Поясните ответ.

_____

_____

Шаг 3: Проверьте новую учетную запись путем входа в рамках сеанса Telnet.

a. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A.

PC-A> **telnet 192.168.1.1**

b. Система запросила у вас учетные данные? Поясните ответ.

_____

Настройте линию vty на использование ранее локально определенных учетных записей и паролей и сконфигурируйте команду **transport input**, чтобы разрешить Telnet.

R1(config)# **line vty 0 4**
R1(config-line)# **login local**
R1(config-line)# **transport input telnet**
R1(config-line)# **exit**

c. Повторно свяжитесь с маршрутизатором R1 с компьютера PC-A с помощью Telnet. PC-A> **telnet 192.168.1.1**

Система запросила у вас учетные данные? Поясните ответ.

_____

d. Войдите в систему как пользователь **user01** с паролем **user01pass**.
e. Во время сеанса Telnet с маршрутизатором R1 войдите в привилегированный режим с помощью команды **enable**.

Какой пароль вы использовали?

_____

f. Для дополнительной безопасности настройте порт AUX на использование локально определенных учетных записей для входа.

R1(config)# **line aux 0**
R1(config-line)# **login local**

g. Завершите сеанс Telnet с помощью команды **exit**.

Шаг 4: Сохраните конфигурацию на маршрутизаторе R1.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

R1# **copy running-config startup-config**

Шаг 5: Выполните шаги 1–4 на маршрутизаторе R3 и сохраните конфигурацию.

Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

Часть 3: Настройка локальной аутентификации на маршрутизаторе R3 с помощью AAA

Задача 1: Настройка локальной базы данных пользователей с помощью Cisco IOS.

Шаг 1: Настройте локальную базу данных пользователей.

a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хеширования SCRYPT.

R3(config)# **username Admin01 privilege 15 algorithm-type scrypt secret Admin01pass**

b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать пароль пользователя?

_____

Задача 2: Настройка локальной аутентификации AAA с помощью Cisco IOS.

Включите сервисы на маршрутизаторе R3 с помощью команды **aaa new-model** в режиме глобальной настройки. Так как вы устанавливаете локальную аутентификацию, используйте ее в качестве первичного метода и метод без аутентификации – в качестве вторичного.

Если вы использовали метод аутентификации через удаленный сервер, например TACACS+ или RADIUS, вы должны были настроить вторичный метод аутентификации в качестве запасного, если сервер недоступен. Обычно вторичным методом является аутентификация по локальной базе данных. В нашем случае, если в локальной базе данных не настроены имена пользователей, маршрутизатор будет предоставлять доступ к устройству всем пользователям.

Шаг 1: Включите сервисы AAA.

R3(config)# **aaa new-model**

Шаг 2: Разверните сервисы AAA с помощью локальной базы данных.

a. Настройте список аутентификации для входа в систему по умолчанию с помощью команды **aaa authentication login default** *method1[method2][method3];* укажите список методов с помощью ключевых слов **local** и **none.**

R3(config)# **aaa authentication login default local-case none**

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Примечание. Параметр **local-case** используется для того, чтобы сделать имена пользователей зависимыми от регистра.

b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R3 con0 is now available

Press RETURN to get started.

Войдите в консоль как **Admin01** с паролем **Admin01pass.** Помните, что сейчас и имена пользователей, и пароли чувствительны к регистру. Вам удалось войти? Поясните ответ.

_____

_____

Примечание. Если ваш сеанс через порт консоли маршрутизатора истекает по времени, вам может потребоваться войти в систему с помощью списка методов аутентификации по умолчанию.

c. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R3 con0 is now available

Press RETURN to get started.

d. Попытайтесь войти в консоль как пользователь **baduser** с любым паролем. Вам удалось войти? Поясните ответ.

_____

_____

Если в локальной базе данных учетные записи пользователей не настроены, каким пользователям будет предоставлен доступ к устройству?

_____

Шаг 3: Создайте профиль аутентификации AAA для Telnet с помощью локальной базы данных.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного метода без аутентификации, поэтому если в локальной базе данных не будет имен пользователей, доступ по Telnet будет отключен. Для создания профиля аутентификации, который не является профилем по умолчанию, укажите имя списка TELNET_LINES и примените его к линиям vty.

```
R3(config)# aaa authentication login TELNET_LINES local
R3(config)# line vty 0 4
R3(config-line)# login authentication TELNET_LINES
```

b. Убедитесь, что профиль аутентификации используется при открытии сеанса Telnet с компьютера PC-C на маршрутизатор R3.

```
PC-C> telnet 192.168.3.1
Trying 192.168.3.1 ... Open
```

c. Войдите как **Admin01** с паролем **Admin01pass.** Вам удалось войти? Поясните ответ.

_____

_____

Завершите сеанс Telnet с помощью команды **exit**, затем снова подключитесь к маршрутизатору R3 по Telnet.

d. Попытайтесь войти как **baduser** с любым паролем. Вам удалось войти? Поясните ответ.

_____

_____

Задача 3: Изучение отладки аутентификации AAA с помощью Cisco IOS.

В этом задании с помощью команды **debug** вы рассмотрите успешные и неуспешные попытки аутентификации.

Шаг 1: Убедитесь, что системное время и временные метки для отладки правильно настроены.

a. От имени пользователя маршрутизатора R3 или в привилегированном режиме введите команду **show clock,** чтобы определить, какое текущее время установлено на маршрутизаторе. Если время и дата установлены неправильно, установите их в привилегированном режиме по команде **clock**

set HH:MM:SS DD month YYYY. Ниже приведен пример для маршрутизатора R3.

R3# **clock set 14:15:00 13 September 2019**

b. Убедитесь, что подробная информация о временных метках доступна в выходных данных отладки, с помощью команды **show run.** Эта команда отобразит все строки текущей конфигурации, в которых есть текст timestamps (временные метки).

R3# **show run | include timestamps**

service timestamps debug datetime msec service timestamps log datetime msec

c. Если команда **service timestamps debug** отсутствует, введите ее в режиме глобальной настройки.

R3(config)# **service timestamps debug datetime msec**

R3(config)# **exit**

d. Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированном режиме.

R3# **copy running-config startup-config**

Шаг 2: Используйте отладку для проверки доступа пользователя.

a. Включите отладку для аутентификации AAA.

R3# **debug aaa authentication**

AAA Authentication debugging is on

b. Запустите на маршрутизаторе R2 сеанс Telnet с маршрутизатором R3.

c. Войдите под именем пользователя **Admin01** и паролем **Admin01pass**. Просмотрите события аутентификации AAA в окне сеанса консоли. Там должны отображаться сообщения об отладке, похожие на следующие.

R3#

Feb 20 08:45:49.383: AAA/BIND(0000000F): Bind i/f

Feb 20 08:45:49.383: AAA/AUTHEN/LOGIN (0000000F): Pick method list 'TELNET_LINES'

d. Из окна Telnet перейдите в привилегированный режим. Используйте пароль привилегированного доступа **cisco12345**. Там должны отображаться сообщения об отладке, похожие на следующие. Обратите внимание на имя пользователя в третьей строке (Admin01), номер виртуального порта (tty132) и адрес удаленного клиента Telnet (10.2.2.2). Также обратите внимание, что последняя строка о состоянии – PASS.

R3#

Feb 20 08:46:43.223: AAA: parse name=tty132 idb type=-1 tty=-1

Feb 20 08:46:43.223: AAA: name=tty132 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=132 channel=0

Feb 20 08:46:43.223: AAA/MEMORY: create_user (0x32716AC8) user='Admin01' ruser='NULL' ds0=0 port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)

Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): port='tty132' list='' action=LOGIN service=ENABLE

Feb 20 08:46:43.223: AAA/AUTHEN/START (2

R3#655524682): non-console enable - default to enable password

Feb 20 08:46:43.223: AAA/AUTHEN/START (2655524682): Method=ENABLE

Feb 20 08:46:43.223: AAA/AUTHEN (2655524682): status = GETPASS

R3#

Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): continue_login (user='(undef)')

Feb 20 08:46:46.315: AAA/AUTHEN (2655524682): status = GETPASS

Feb 20 08:46:46.315: AAA/AUTHEN/CONT (2655524682): Method=ENABLE

Feb 20 08:46:46.543: AAA/AUTHEN (2655524682): status = PASS

e. В окне Telnet выйдите из привилегированного режима с помощью команды **disable.** Попытайтесь перейти в привилегированный режим снова, но на этот раз используйте неправильный пароль. Просмотрите выходные данные отладчика на маршрутизаторе R3. Обратите внимание, что сейчас состояние – FAIL.

Feb 20 08:47:36.127: AAA/AUTHEN (4254493175): status = GETPASS

Feb 20 08:47:36.127: AAA/AUTHEN/CONT (4254493175): Method=ENABLE

Feb 20 08:47:36.355: AAA/AUTHEN(4254493175): password incorrect

Feb 20 08:47:36.355: AAA/AUTHEN (4254493175): status = FAIL

Feb 20 08:47:36.355: AAA/MEMORY: free_user (0x32148CE4) user='NULL' ruser='NULL' port='tty132' rem_addr='10.2.2.2' authen_type=ASCII service=ENABLE priv=15 vrf= (id=0)

R3#

f. В окне Telnet выйдите из сеанса Telnet с маршрутизатором. Попытайтесь снова открыть сеанс Telnet с маршрутизатором, но на этот раз попытайтесь войти в систему как **Admin01** с неправильным паролем. Выходные данные отладчика в окне консоли должны быть похожи на следующее.

Feb 20 08:48:17.887: AAA/AUTHEN/LOGIN (00000010): Pick method list 'TELNET_LINES' Какое сообщение было показано на экране клиента Telnet?

_____

_____

Выключите полностью процесс отладки с помощью команды привилегированного режима **undebug all.**

Часть 4: Настройка централизованной аутентификации с помощью AAA и RADIUS

В части 4 данной лабораторной работы необходимо установить программное обеспечение RADIUS на компьютере PC-A. Затем необходимо настроить доступ на маршрутизаторе R1 к внешнему серверу RADIUS для

аутентификации пользователей. В этой части лабораторной работы используется бесплатный сервер WinRadius.

Задача 1: Восстановление базовой конфигурации маршрутизатора R1.

Чтобы избежать ошибок из-за созданной ранее конфигурации AAA RADIUS, начните с возврата базовых настроек на маршрутизаторе R1, как показано в частях 1 и 2 данной лабораторной работы.

Шаг 1: Повторно загрузите и восстановите сохраненную конфигурацию на маршрутизаторе R1.

На данном шаге верните базовые настройки на маршрутизаторе, сохраненные в частях 1 и 2.

a. Подключитесь к консоли маршрутизатора R1, войдите в систему как **user01** с паролем **user01pass.**
b. Войдите в привилегированный режим с паролем **cisco12345.**
c. Перезагрузите маршрутизатор и ответьте **no** на запрос о сохранении конфигурации.

R1# **reload**
System configuration has been modified. Save? [yes/no]: **no**
Proceed with reload? [confirm]

Шаг 2: Проверьте связь.

a. Проверьте связь, отправив эхо-запрос с компьютера PC-A на PC-C. Если запрос выполнился с ошибкой, устраните неисправности в настройках маршрутизатора и ПК.
b. Если вы вышли из консоли, войдите снова как **user01** с паролем **user01pass**, затем войдите в привилегированный режим с паролем **cisco12345.**

Задача 2: Загрузка и установка на компьютере PC-A сервера RADIUS.

Существует несколько серверов RADIUS, как платных, так и бесплатных. В данной лабораторной работе используется WinRadius – стандартный бесплатный сервер RADIUS, работающий под управлением ОС Windows. Бесплатная версия этого ПО поддерживает лишь 5 имен пользователей.

Примечание. Zip-архив с программным обеспечением WinRadius можно запросить у своего инструктора.

Шаг 1: Загрузите программное обеспечение WinRadius.

a. Создайте папку с именем **WinRadius** на рабочем столе или в другом месте, куда будете сохранять файлы.
b. Распакуйте архив с WinRadius в папку, созданную на шаге 1a. Среди них не будет файла с установщиком. Распакованный файл WinRadius.exe является исполняемым.
c. На рабочем столе можно создать ярлык для файла WinRadius.exe. **Примечание.** Если WinRadius используется на компьютере под управлением ОС Microsoft Windows Vista или Microsoft Windows 7, есть вероятность, что

интерфейс ODBC (Open Database Connectivity) не будет создан, так как он не сможет записывать данные в реестр.

Возможные решения:

a. Настройки для Compatibility (совместимость)

1) Щелкните правой кнопкой мыши значок **WinRadius.exe** и выберите **Properties**.
2) В диалоговом окне **Properties** перейдите на вкладку **Compatibility.** На этой вкладке установите флажок **Run this program in compatibility mode for**. Затем в раскрывающемся меню снизу выберите установленную на вашем компьютере операционную систему (например, Windows 7).
3) Нажмите **ОК.**

b. Настройки для Run as Administrator

1) Щелкните правой кнопкой мыши значок **WinRadius.exe** и выберите **Properties**.
2) В диалоговом окне **Properties** перейдите на вкладку **Compatibility.** На этой вкладке установите флажок **Run this program as administrator** в разделе Privilege Level.
3) Нажмите **ОК.**

c. Выберите Run as Administration для каждого запуска

1) Щелкните правой кнопкой значок **WinRadius.exe** и выберите **Run as Administrator**.
2) После запуска ПО WinRadius нажмите **Yes** в диалоговом окне User Account Control.

Шаг 2: Настройте базу данных сервера WinRadius.

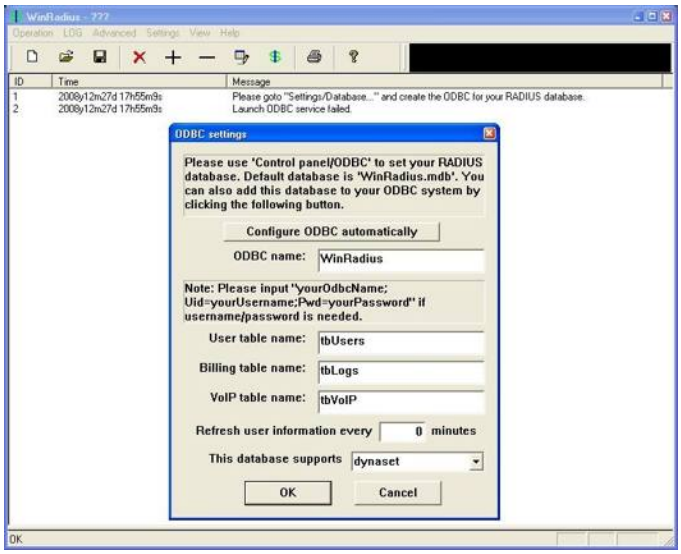
a. Запустите приложение WinRadius.exe**.** WinRadius использует локальную базу данных для хранения информации о пользователях. При первом запуске приложения появятся следующие сообщения:

Please go to “Settings/Database and create the ODBC for your RADIUS database.

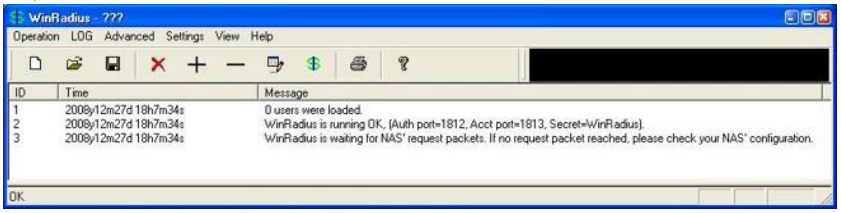
Launch
ODBC failed.

b. В главном меню выберите **Settings > Database.** Появится следующий экран. Нажмите кнопку **Configure ODBC Automatically,** затем нажмите **OK.** Вы должны получить сообщение, что ODBC был создан успешно.

Выйдите из WinRadius и перезапустите приложение, чтобы применить изменения.



c. При повторном запуске WinRadius вы должны увидеть следующие сообщения.



Шаг 3: Настройте пользователей и пароли на сервере WinRadius.

a. В главном меню выберите **Operation** > **Add User**.

b. Введите имя пользователя **RadUser** и пароль **RadUserpass.** Помните, что пароли чувствительны к регистру.

c. Нажмите **ОК.** Вы должны получить сообщение в окне журнала о том, что пользователь успешно добавлен.

Шаг 4: Очистите окно журнала.

В главном меню выберите **Log** > **Clear**.

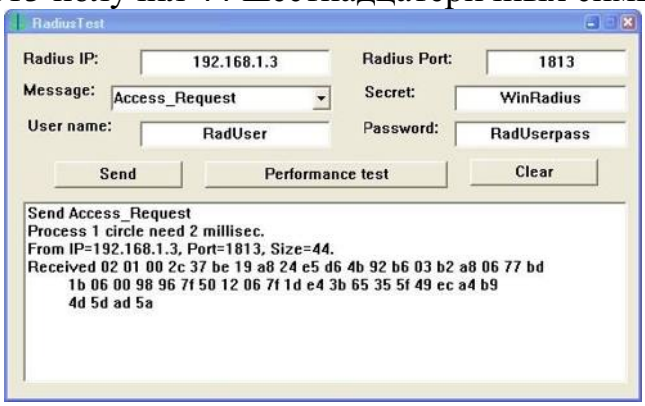
Шаг 5: Проверьте только что добавленного пользователя с помощью утилиты тестирования WinRadius.

a. В скачанном архиве находится утилита тестирования WinRadius. Перейдите в папку, куда вы распаковали WinRadius.zip, и найдите файл RadiusTest.exe.

Запустите приложение RadiusTest, введите IP-адрес сервера RADIUS (**192.168.1.3),** имя пользователя **RadUser** и пароль **RadUserpass,** как

показано ниже. Не изменяйте номер порта RADIUS по умолчанию 1813 и пароль RADIUS **WinRadius.**

b. Нажмите **Send**, после чего вы должны увидеть сообщение Send Access_Request, в котором будет указано, что сервер по адресу 192.168.1.3 через порт 1813 получил 44 шестнадцатеричных символа.



c. Просмотрите журнал WinRadius и убедитесь, что пользователь RadUser был успешно аутентифицирован.

Задача 3: Настройка на маршрутизаторе R1 сервисов AAA и получение доступа к серверу RADIUS с помощью Cisco IOS.

Шаг 1: Включите AAA на маршрутизаторе R1.

Воспользуйтесь командой **aaa new-model** в режиме глобальной настройки, чтобы включить AAA.

R1(config)# **aaa new-model**

Шаг 2: Настройте список методов аутентификации при входе в систему по умолчанию.

a. Настройте список на первоочередное использование RADIUS для сервиса аутентификации, а далее – без аутентификации. Если сервер RADIUS недоступен и аутентификация не может быть выполнена, маршрутизатор глобально разрешает доступ без аутентификации. Это необходимо для случая, если маршрутизатор начнет работу без связи с активным сервером RADIUS.

R1(config)# **aaa authentication login default group radius none**

b. В качестве альтернативы вы можете настроить локальную аутентификацию в качестве запасного метода.

Примечание. Если вы не укажете список методов аутентификации по умолчанию, маршрутизатор может быть заблокирован, и вам будет нужно выполнить процедуру восстановления пароля для конкретного маршрутизатора.

Шаг 3: Укажите сервер RADIUS.

a. Используйте команду **radius server** для входа в режим настройки сервера RADIUS.

R1(config)# **radius server CCNAS**

b. Используйте символ ? для вывода списка команд подрежима для настройки сервера RADIUS.

R1(config-radius-server)# ?

RADIUS server sub-mode commands:
address Specify the radius server address
automate-tester Configure server automated
testing.
backoff Retry backoff pattern(Default is retransmits
with constant delay) exit Exit from
RADIUS server configuration mode key Per-
server encryption key no Negate a command or
set its defaults non-standard Attributes to be parsed that
violate RADIUS standard pac Protected Access
Credential key retransmit Number of retries to active
server (overrides default) timeout Time to wait (in
seconds) for this radius server to reply
(overrides default)

c. Используйте команду **address** для настройки IP-адреса для компьютера PC-A.
R1(config-radius-server)# **address ipv4 192.168.1.3**
d. Команда **key** используется для установки секретного пароля, который является общим для сервера RADIUS и маршрутизатора (в данном случае R1) и применяется для аутентификации соединения между маршрутизатором и сервером прежде, чем начнется процесс аутентификации пользователя. Используйте секретный пароль NAS по умолчанию **WinRadius,** указанный на сервере RADIUS (см. задачу 2, шаг 5). Помните, что пароли чувствительны к регистру.
R1(config-radius-server)# **key WinRadius**
R1(config-redius-server)# **end**

Задача 4: Проверка конфигурации AAA RADIUS.

Шаг 1: Проверьте связь между маршрутизатором R1 и компьютером, на котором работает сервер RADIUS.

Отправьте эхо-запрос с маршрутизатора R1 на компьютер PC-A.
R1# **ping 192.168.1.3**

Если запрос выполнен с ошибкой, проведите диагностику основных настроек компьютера и маршрутизатора перед тем, как продолжить.

Шаг 2: Проверьте конфигурацию.

a. Если вы перезапускали сервер WinRadius, вам потребуется заново создать пользователя **RadUser** с паролем **RadUserpass** путем выбора **Operation** > **Add User**.
b. Очистите журнал на сервере WinRadius путем выбора **Log** > **Clear** в главном меню.
c. На маршрутизаторе R1 перейдите на начальный экран маршрутизатора, на котором отображается:
R1 con0 is now available
Press RETURN to get started.

d. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя имя пользователя **RadUser** и пароль **RadUserpass.** Удалось ли вам получить доступ в привилегированный режим и если да, была ли задержка?

_____

Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:
R1 con0 is now available
Press RETURN to get started.

e. Проверьте конфигурацию – войдите в консоль на маршрутизаторе R1, используя несуществующее имя пользователя **Userxxx** и пароль **Userxxxpass.** Удалось ли вам получить доступ в привилегированный режим? Поясните ответ.

_____

_____

Были ли отображены какие-либо сообщения в журнале сервера RADIUS или при входе? _____

f. Почему несуществующему пользователю удалось получить доступ к маршрутизатору и при этом не были выведены сообщения в журнале сервера RADIUS?

_____

_____

Когда сервер RADIUS недоступен, после попыток входа в систему могут появляться примерно следующие сообщения:
*Dec 26 16:46:54.039: %RADIUS-4-RADIUS_DEAD: RADIUS server 192.168.1.3:1645,1646 is not responding.
*Dec 26 15:46:54.039: %RADIUS-4-RADIUS_ALIVE: RADIUS server 192.168.1.3:1645,1646 is being marked alive.

Шаг 3: Устраните неполадки при связи между маршрутизатором и сервером RADIUS.

a. Проверьте номера портов Cisco IOS RADIUS UDP по умолчанию, используемые на маршрутизаторе R1: снова войдите в режим настройки сервера RADIUS с помощью команды **radius server**, а затем используйте функцию Cisco IOS Help в команде подрежима **address.**
R1(config)# **radius server CCNAS**
R1(config-radius-server)# **address ipv4 192.168.1.3 ?**
acct-port UDP port for RADIUS acco/unting server (default is 1646) alias 1-8 aliases for this server (max. 8) auth-port UDP port for RADIUS authentication server (default is 1645) <cr>
Каковы номера портов Cisco IOS UDP по умолчанию маршрутизатора R1 для сервера RADIUS?

_____

Шаг 4: Проверьте номера портов по умолчанию на сервере WinRadius на компьютере PC-A.

В главном меню WinRadius выберите **Settings > System.**

Каковы номера портов WinRadius UDP по умолчанию?

_____

Примечание. В документе RFC 2865 официально назначены номера портов 1812 и 1813 для RADIUS.

Шаг 5: Поменяйте номера портов RADIUS на маршрутизаторе R1 для соответствия с сервером WinRadius.

Если не указано иное, конфигурация Cisco IOS RADIUS по умолчанию настроена на номера портов UDP 1645 и 1646. Либо номера портов Cisco IOS должны быть изменены в соответствии с номерами портов сервера RADIUS, либо номера портов сервера RADIUS должны быть изменены в соответствии с номерами портов маршрутизатора Cisco IOS. Снова введите команду подрежима address. На этот раз укажите номера портов **1812** и **1813,** а также адрес IPv4.

R1(config-radius-server)# **address ipv4 192.168.1.3 auth-port 1812 acct-port 1813**

Шаг 6: Проверьте конфигурацию, войдя в консоль на маршрутизаторе R1.

a. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться: R1 con0 is now available, Press **RETURN** to get started.
b. Снова войдите под именем **RadUser** и паролем **RadUserpass.** Вам удалось войти? Была ли задержка на этот раз?

_____

_____

В журнале на сервере RADIUS должно появиться следующее сообщение.

User (RadUser) authenticate OK.

c. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:

R1 con0 is now available, Press RETURN to get started.

d. Снова войдите с именем **Userxxx** и паролем **Userxxxpass.** Вам удалось войти?

_____

_____

Какое сообщение появилось на маршрутизаторе?

_____

В журнале на сервере RADIUS должны появиться следующие сообщения.

Reason: Unknown username

User (Userxxx) authenticate failed

Шаг 7: Создайте список методов аутентификации для Telnet и протестируйте его.

a. Создайте отдельный список методов аутентификации для доступа к маршрутизатору по Telnet. В нем не должно быть запасного режима «без аутентификации», поэтому если доступ к серверу RADIUS отсутствует, то доступ по Telnet будет отключен. Назовите данный список **TELNET_LINES**.
   R1(config)# **aaa authentication login TELNET_LINES group radius**
b. Примените список к линиям vty на маршрутизаторе, используя команду login authentication.
   R1(config)# **line vty 0 4**
   R1(config-line)# **login authentication TELNET_LINES**
c. Подключитесь с компьютера PC-A к маршрутизатору R1 по Telnet и войдите с именем **RadUser** и паролем **RadUserpass.** Вам удалось получить доступ для входа? Поясните ответ.

   _____

   _____

d. Завершите сеанс Telnet, затем снова с компьютера PC-A подключитесь к маршрутизатору R1 по Telnet. Войдите с именем **Userxxx** и паролем **Userxxxpass.** Вам удалось войти? Поясните ответ.

_____

_____

Критерии оценивания практической работы

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ТЕМА 7. КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ

УСТНЫЙ ОПРОС ПО ТЕМЕ «КРИПТОГРАФИЧЕСКИЕ СИСТЕМЫ»

Вопросы:

1. Криптографические сервисы.
2. Базовая целостность и аутентичность.
3. Конфиденциальность.
4. Криптография открытых ключей.

Критерии оценки устного ответа

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА ИССЛЕДОВАНИЕ МЕТОДОВ ШИФРОВАНИЯ

1. Цель работы

Знакомство с основными методами криптографической зашиты информации.

2. Краткие теоретические сведения

Криптография – обеспечивает сокрытие смысла сообщения с помощью шифрования и открытия его расшифровкой, которые выполняются по специальным алгоритмам с помощью ключей.

Ключ – конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма.

Криптоанализ – занимается вскрытием шифра без знания ключа (проверка устойчивости шифра).

Кодирование – (не относится к криптографии) – система условных обозначений, применяемых при передаче информации. Применяется для увеличения качества передачи информации, сжатия информации и для уменьшения стоимости хранения и передачи.

Криптографические преобразования имеют цель обеспечить недоступность информации для лиц, не имеющих ключа, и поддержание с требуемой надежностью обнаружения несанкционированных искажений.

Большинство средств защиты информации базируется на использовании криптографических шифров и процедур шифрования-расшифровки. В соответствии со стандартом ГОСТ 28147-89 под **шифром** понимают совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, задаваемых ключом и алгоритмом преобразования.

В криптографии используются следующие основные алгоритмы шифрования:

- алгоритм замены (подстановки) – символы шифруемого текста заменяются символами того же или другого алфавита в соответствии с заранее обусловленной схемой замены;
- алгоритм перестановки – символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста;
- гаммирование – символы шифруемого текста складываются с символами некоторой случайной последовательности;
- аналитическое преобразование – преобразование шифруемого текста по некоторому аналитическому правилу (формуле).

Процессы шифрования и расшифровки осуществляются в рамках некоторой криптосистемы. Для **симметричной** криптосистемы характерно применение одного и того же ключа как при шифровании, так и при расшифровке сообщений. В **асимметричных** криптосистемах для шифрования данных используется один (общедоступный) ключ, а для расшифровки – другой (секретный) ключ.

Симметричные криптосистемы

Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение “Неясное становится еще более непонятным” записывается в таблицу из 5 строк и 7 столбцов по столбцам:

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ НЯЕЕО ЯОЕТЯ СВЕЛП НСТИЩ ЕОЫНА ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает **метод одиночной перестановки** по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору

чисел длиной в строку таблицы. Используя в качестве ключа слово «ЛУНАТИК», получим следующую таблицу:

Л	У	Н	А	Т	И	К
4	7	5	1	6	2	3
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

А	И	К	Л	Н	Т	У
1	2	3	4	5	6	7
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН БОЯЕТ ЕООЕЕ ПНЯВЛ СЩОЫС ИЕТЕН МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются **алгоритмы двойных перестановок**. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке перестановки проводятся в обратном порядке. Например, сообщение “Приезжаю_шестого” можно зашифровать следующим образом:

	2	4	1	3			1	2	3	4			1	2	3	4
4	П	Р	И	Е		4	И	П	Е	Р		1	А	З	Ю	Ж
1	З	Ж	А	Ю		1	А	З	Ю	Ж		2	Е	_	С	Ш
2	_	Ш	Е	С		2	Е.	_	С	Ш		3	Г	Т	О	О
3	Т	О	Г	О		3	Г	Т	О	О		4	И	П	Е	Р

Двойная перестановка столбцов и строк

В результате перестановки получена шифровка АЗЮЖЕ_СШГТООИПЕР. Ключом к шифру служат номера столбцов 2413 и номера строк 4123 исходной таблицы.

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 х 3 их 36, для 4 х 4 их 576, а для 5*5 их 14400.

В средние века для шифрования применялись и **магические квадраты**. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведенной в квадрате нумерации и затем переписать содержимое таблицы по строкам. В результате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

16	3	2	13			О	И	Р	Т
5	10	11	8			З	Ш	Е	Ю
9	6	7	12			_	Ж	А	С
4	15	14	1			Е	Г	О	П

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы 3*3 таких квадратов -1; для таблицы 4*4 - 880; а для таблицы 5*5-250000.

Шифры простой замены

Система шифрования Цезаря - частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый **полибианский квадрат** размером 5*5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда

Сообщение: СОВЕРШЕННО СЕКРЕТНО

Ключ: 3143143143143143

Шифровка: ФПИСЬИОССАХИЛФИУСС

В **шифрах многоалфавитной замены** для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит):

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭ
.	……
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЧШЩЪЫЬЭЮЯ_А

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы по букве текста и строке, соответствующей букве ключа. Например, используя ключ АГАВА, из сообщения ПРИЕЗЖАЮ ШЕСТОГО получаем следующую шифровку:

Сообщение	ПРИЕЗЖАЮ_ШЕСТОГО
Ключ	АГАВААГАВААГАВАА
Шифровка	ПНИГЗЖЮЮЮАЕОТМГО

Гаммирование

Процесс шифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $Т(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины ($Т(ш)_i$=$Г(ш)_i$+$Т(0)_i$, где + - побитовое сложение, i =1-m).

Процесс расшифровки сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $Т(0)_i$=$Г(ш)_i$+$Т(ш)_i$.

Асимметричные криптосистемы

Схема шифрования Эль Гамаля

Алгоритм шифрования Эль Гамаля основан на применении больших чисел для генерации открытого и закрытого ключа, криптостойкость же обусловлена сложностью вычисления дискретных логарифмов.

Последовательность действий пользователя:

1. Получатель сообщения выбирает два больших числа P и G, причем $P > G$.
2. Получатель выбирает секретный ключ - случайное целое число $X < P$.
3. Вычисляется открытый ключ $Y = G^X \bmod P$.
4. Получатель выбирает целое число K, $1 < K < P-1$.
5. Шифрование сообщения (M): $a = G^K \bmod P$, $b = Y^K M \bmod P$, где пара чисел (a,b) является шифротекстом.

Криптосистема шифрования данных RSA

Предложена в 1978 году авторами Rivest, Shamir и Aldeman и основана на трудности разложения больших целых чисел на простые сомножители.

Алгоритм создания открытого и секретного ключей:

1. Получатель выбирает 2 больших простых целых числа p и q, на основе которых вычисляет $n=p*q$ и функцию Эйлера $\varphi(n)=(p-1)(q-1)$.
2. Получатель выбирает целое число e ($1<e<\varphi(n)$), взаимно простое со значением функции $\varphi(n)$.

Пара чисел **(e,n)** публикуется в качестве **открытого ключа**.

3. Получатель вычисляет целое число d, которое отвечает условию: $e*d=1 \pmod{\varphi(n)}$.

Пара чисел **(d,n)** является **секретным ключом**.

Шифрование сообщения с использованием открытого ключа:

Если m – сообщение (сообщениями являются целые числа в интервале от 0 до n-1), то зашифровать это сообщение можно как $\mathbf{c=m^e \bmod(n)}$.

Дешифрование сообщения с использованием секретного ключа:

Получатель расшифровывает, полученное сообщение c: $\mathbf{m=c^d \bmod(n)}$.

3. Задание

Практическая работа состоит из двух частей:

Часть 1 – применение одного из алгоритмов симметричного шифрования;

Часть 2 – шифрование с использованием алгоритма RSA.

Порядок выполнения работы:

Часть 1:

1. Используя один из алгоритмов симметричного шифрования (см. вариант), зашифровать свои данные: фамилию, имя, отчество.
2. Выполнить проверку, расшифровав полученное сообщение.

Часть 2:

1. Написать программу, реализующую алгоритм шифрования и дешифрования сообщения RSA. Входные данные: открытый и секретный ключи (значения n, e, d) и сообщение (m).

2. Используя заданные значения p, q, e, d (см. вариант) зашифровать и дешифровать сообщения m_1, m_2, m_3 (см. вариант).

4. Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Применение алгоритма симметричного шифрования
5. Применение алгоритма асимметричного шифрования
   5.1. Программа шифрования и дешифрования сообщения при помощи алгоритма RSA
   5.2. Результаты шифрования и дешифрования заданных сообщений
6. Выводы

5. Варианты

Вариант – номер по списку в журнале.

Номер варианта	**Исходные данные**							
	Часть 1	**Часть 2**						
	Алгоритм шифрования	**p**	**q**	**e**	**d**	**m_1**	**m_2**	**m_3**
1	Простая перестановка	3	11	7	3	9	12	23
3	Одиночная перестановка	17	11	7	23	8	15	45
3	Двойная перестановка	13	7	5	29	3	16	55
4	Магический квадрат	101	113	3533	6597	6	19	23
5	Шифр Цезаря	7	11	37	13	8	18	51
6	Полибианский квадрат	7	17	5	77	9	11	86
7	Шифр Гронсфельда	3	11	7	3	8	13	25
8	Многоалфавитная замена	17	11	7	23	7	14	47
9	Простая перестановка	13	7	5	29	2	17	55
10	Одиночная перестановка	17	11	7	23	3	20	51
11	Двойная перестановка	13	7	5	29	2	12	15
12	Магический квадрат	101	113	3533	6597	3	15	86
13	Шифр Цезаря	7	11	37	13	3	16	54
14	Полибианский квадрат	7	17	5	77	3	19	36
15	Шифр Гронсфельда	3	11	7	3	4	18	25
16	Многоалфавитная замена	17	11	7	23	5	11	64
17	Простая перестановка	101	113	3533	6597	4	13	91
18	Одиночная перестановка	7	11	37	13	7	14	34
19	Двойная перестановка	7	17	5	77	7	17	73
20	Магический квадрат	3	11	7	3	5	20	23
21	Шифр Цезаря	17	11	7	23	2	11	85
22	Полибианский квадрат	13	7	5	29	3	13	57
23	Шифр Гронсфельда	17	11	7	23	2	14	59
24	Многоалфавитная замена	13	7	5	29	5	17	56
25	Простая перестановка	101	113	3533	6597	6	20	92

26	Одиночная перестановка	7	11	37	13	5	14	76
27	Двойная перестановка	7	17	5	77	4	17	64
28	Магический квадрат	3	11	7	3	8	20	32
29	Одиночная перестановка	7	17	5	77	4	13	91
30	Шифр Гронсфельда	13	7	5	29	9	11	58

Критерии оценивания практической работы

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

ТЕМА 8. РЕАЛИЗАЦИЯ ТЕХНОЛОГИЙ VPN

УСТНЫЙ ОПРОС ПО ТЕМЕ «РЕАЛИЗАЦИЯ ТЕХНОЛОГИЙ VPN»

Вопросы:

1. VPN.
2. GRE VPN.
3. Компоненты и функционирование IPSec VPN.
4. Реализация Site-to-site IPSec VPN с использованием CLI.
5. Реализация Site-to-site IPSec VPN с использованием CCP.
6. Реализация Remote-access VPN.

Критерии оценки устного ответа

«5 (отлично)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, литературным языком: ответ самостоятельный.

«4 (хорошо)»: ответ полный и правильный на основании изученных теорий; материал изложен в определенной логической последовательности, при этом допущены две-три несущественные ошибки, исправленные по требованию преподавателя.

«3 (удовлетворительно)»: ответ полный, но при этом допущена существенная ошибка, или неполный, несвязный.

«2 (неудовлетворительно)»: при ответе обнаружено непонимание студентом основного содержания учебного материала или допущены существенные ошибки, которые студент не смог исправить при наводящих вопросах преподавателя.

ПРАКТИЧЕСКАЯ РАБОТА НАСТРОЙКА SITE-TO-SITEVPN ИСПОЛЬЗУЯ ИНТЕРФЕЙС КОМАНДНОЙ СТРОКИ

Топология

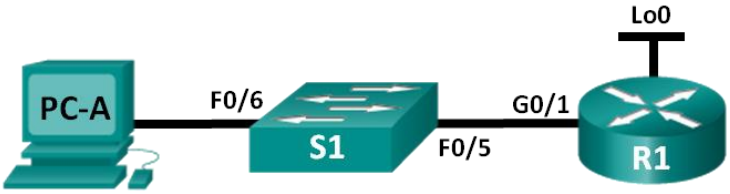


Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
	Lo0	209.165.200.225	255.255.255.224	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1: настройте топологию и инициализацию устройств

- Настройте оборудование в соответствии с топологией сети.
- Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.

Часть 2: настройте параметры устройств и проверьте надёжность подключения

- Присвойте статический IP-адрес маршрутизатору PC-A NIC.
- Настройте базовые параметры на маршрутизаторе R1.
- Выполните базовую настройку коммутатора S1.
- Проверьте подключение к сети.

Часть 3: соберите сведения о сетевых устройствах

- Соберите информацию на R1 с помощью команд IOS CLI.
- Соберите информацию на S1 с помощью команд IOS CLI.
- Соберите информацию на PC-A с помощью команды CLI.

Исходные данные/сценарий

Одна из наиболее важных задач, выполняемых специалистами в области вычислительных сетей, состоит в документировании работы сети. Наличие документации, относящейся к IP-адресам, номерам моделей, версиями IOS, используемым портам и результатам проверки безопасности, имеет большое значение при поиске и устранении неполадок в работе сети.

В этой лабораторной работе вы построите небольшую вычислительную сеть, выполните настройку устройств, добавите некоторые основные средства защиты, а затем создадите документацию для полученной конфигурации, выполняя на маршрутизаторе, коммутаторе и ПК различные команды для сбора требуемой информации.

Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением ОС Cisco IOS 15.2(4) M3 (образ universalk9).

В лабораторной работе используются коммутаторы серии Cisco Catalyst 2960s под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.

Примечание. Убедитесь, что предыдущие настройки маршрутизаторов и коммутаторов удалены, и они не имеют загрузочной конфигурации. Если вы не уверены в этом, обратитесь к преподавателю.

Необходимые ресурсы:

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичный)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- 1 ПК (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
- консольные кабели для настройки устройств Cisco IOS через порты консоли;
- кабели Ethernet, расположенные в соответствии с топологией.

Часть 1: Настройка топологии и инициализация устройств

В первой части лабораторной работы вам предстоит создать топологию сети, при необходимости удалить все настройки и настроить основные параметры для маршрутизатора и коммутатора.

Шаг 1: Подключите кабели в сети в соответствии с топологией.

a. Подключите устройства, как показано в топологии, и подсоедините необходимые кабели.
b. Включите все устройства в топологии.

Шаг 2: Выполните запуск и перезагрузку маршрутизатора и коммутатора.

Часть 2: Настройка устройств и проверка подключения

Во второй части лабораторной работы вам предстоит создать топологию сети и настроить основные параметры для маршрутизатора и коммутатора. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.

Примечание. В приложении A приведены сведения о конфигурации для выполнения шагов в части 2. Постарайтесь выполнить часть 2, не пользуясь приложением.

Шаг 1: Настройте IPv4-адрес на ПК.

На основе таблицы адресации настройте адрес IPv4, маску подсети и адрес шлюза по умолчанию для PC-A.

Шаг 2: Настройте маршрутизатор.

Если возникли трудности при выполнении шага 2, обратитесь к приложению А.

a. Подключите консоль к маршрутизатору и войдите в привилегированный режим EXEC.
b. Установите на маршрутизаторе правильные время и дату.
c. Войдите в режим глобальной конфигурации.

1) На основе топологии и таблицы адресации присвойте маршрутизатору имя устройства.
2) Отключите поиск DNS.
3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.
4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
5) Назначьте **cisco** в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.
6) Зашифруйте все открытые пароли.
7) Для доступа с использованием SSH создайте имя домена **cisco.com**.
8) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.
9) Создайте ключ RSA. Для числа битов используйте значение **512**.

d. Настройте доступ к каналу vty.

1) Для аутентификации при использовании SSH настройте локальную базу данных.
2) Активируйте SSH только для доступа с использованием имени для входа.

e. Вернитесь в режим глобальной конфигурации.

1) Создайте интерфейс Loopback 0 и присвойте IP-адрес на основе таблицы адресации.
2) Настройте и активируйте интерфейс G0/1 на маршрутизаторе.
3) Настройте описания интерфейсов для G0/1 и L0.
4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

Шаг 3: Настройте коммутатор.

Если возникли трудности при выполнении шага 3, обратитесь к приложению А.

a. Подключите консоль к коммутатору и войдите в привилегированный режим EXEC.
b. Установите на коммутаторе правильные время и дату.
c. Войдите в режим глобальной конфигурации.

1) На основе топологии и таблицы адресации присвойте коммутатору имя устройства.
2) Отключите поиск DNS.
3) Создайте баннер MOTD с предупреждением о запрете несанкционированного доступа к устройству.

4) Назначьте **class** в качестве зашифрованного пароля привилегированного режима EXEC.
5) Зашифруйте все открытые пароли.
6) Для доступа с использованием SSH создайте имя домена **cisco.com**.
7) Для доступа с использованием SSH создайте пользователя **admin** с секретным паролем **cisco**.
8) Создайте ключ RSA. Для числа битов используйте значение **512**.
9) На основе топологии и таблицы адресации создайте и активируйте на коммутаторе IP-адрес.
10) Установите на коммутаторе шлюз по умолчанию.
11) Назначьте **cisco** в качестве пароля консоли и активируйте использование имени для входа при получении доступа к консоли.

d. Настройте доступ к каналу vty.

1) Для аутентификации при использовании SSH настройте локальную базу данных.
2) Активируйте SSH только для доступа с использованием имени для входа.
3) Войдите в соответствующий режим для настройки описаний интерфейсов для F0/5 и F0/6.
4) Сохраните файл текущей конфигурации в файле загрузочной конфигурации.

Шаг 4: Проверьте подключение к сети.

a. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса коммутатора S1 в сети VLAN 1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.
b. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса шлюза по умолчанию на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.
c. Из командной строки на компьютере PC-A выполните команду ping для IP-адреса интерфейса закольцовывания на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.
d. Снова подключите консоль к коммутатору и выполните команду ping для IP-адреса шлюза G0/1 на маршрутизаторе R1. Если команды ping дали неудовлетворительный результат, отыщите ошибки в физических и логических настройках и выполните требуемые исправления.

Часть 3: Сбор сведений о сетевых устройствах

В части 3 вы будете использовать различные команды для сбора сведений о сетевых устройствах и некоторых рабочих характеристик. Документация со сведениями о вычислительной сети является очень важной составляющей управления сетью. Важно документировать как физическую, так и логическую топологию, а также проверять модели платформ и версии IOS сетевых устройств. Специалистам по вычислительным сетям важно знать соответствующие команды для сбора сведений о сети.

Шаг 1: Соберите информацию на R1 с помощью команд IOS.

Одним из важнейших основных действий является сбор сведений о физическом устройстве наряду со сведениями об операционной системе.

a. Примените соответствующую команду для выявления следующих данных.

Модель маршрутизатора:
Версия IOS:
Всего ОЗУ:
Всего ОЗУ:
Всего флэш-памяти:
Файл-образ IOS:
Реестр конфигурации:
Технологический пакет:
Какая команда используется для сбора информации?

_____

b. Для отображения сводки с важными сведениями об интерфейсах маршрутизаторов используйте соответствующую команду. Ниже запишите команду и полученные результаты.

Примечание. Запишите только те интерфейсы, у которых есть IP-адреса.

_____

_____

_____

c. Примените соответствующую команду для отображения таблицы маршрутизации. Ниже запишите команду и полученные результаты.

_____

_____

Какую команду следует использовать для отображения таблицы сопоставления адресов уровня 2 и уровня 3 на маршрутизаторе? Ниже запишите команду и полученные результаты.

_____

_____

Какую команду следует использовать для просмотра подробных сведений обо всех интерфейсах на маршрутизаторе или о конкретном интерфейсе? Ниже запишите команду.

_____

d. Существует очень мощный протокол Cisco, работающий на уровне 2 модели OSI. Этот протокол облегчит получение схемы физических соединений устройств Cisco, а также определение номеров моделей и даже версий IOS и адресов IP. Какую команду или команды следует использовать на маршрутизаторе R1 для поиска информации о коммутаторе S1 для заполнения следующей таблицы?

Идентификатор устройства	Локальный интерфейс	Возможность настройки	Номер модели	Идентификатор удаленного порта	IP-адрес	Версия IOS

Простейшая проверка сетевых устройств осуществляется с помощью попытки подключиться к ним с использованием протокола telnet. Следует помнить, что Telnet не является безопасным протоколом. В большинстве случаев его не следует активировать. С помощью клиента Telnet, например Tera Term или PuTTY, попытайтесь посредством telnet подключиться к R1 с использованием IP-адреса шлюза по умолчанию. Полученные результаты запишите ниже.

_____

С компьютера PC-A выполните проверку правильности работы SSH. Используя клиент SSH, например Tera Term или PuTTY, подключитесь посредством SSH к маршрутизатору R1 с компьютера PC-A. В случае получения сообщения с предупреждением об отличающемся ключе нажмите кнопку Continue («Продолжить»). Подключитесь с использованием соответствующего имени пользователя и пароля, созданных в части 2. Успешно ли был обработан эхо-запрос?

_____

Различные пароли, настраиваемые на маршрутизаторе, должны быть надёжными и защищёными в максимально возможной степени.

Примечание. Пароли, используемые для нашей лабораторной работы (ciscoи class) не соответствуют общепринятым требованиям для надёжных паролей. Эти пароли используются просто для удобства выполнения лабораторных работ. По умолчанию пароль консоли и все пароли канала vty явно отображаются в вашем файле конфигурации.

Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученные результаты.

Команда: _____

Пароль консоли зашифрован? _____

Пароль SSH зашифрован? _____

Шаг 2: Соберите информацию на S1 с помощью команд IOS.

Многие из команд, используемых на маршрутизаторе R1, можно применять также на коммутаторе. Однако между некоторыми из этих команд существуют определённые различия.

Примените соответствующую команду для выявления следующих данных.

Модель коммутатора:

Версия IOS:

Всего RAM:

Файл-образ IOS:

Какая команда используется для сбора информации?

_____

Для отображения сводки с важными сведениями об интерфейсах коммутаторов используйте соответствующую команду. Ниже запишите команду и полученные результаты.

Примечание. Укажите только активные интерфейсы.

_____

Примените соответствующую команду для отображения таблицы MAC-адресов коммутатора. В отведённом ниже месте запишите только MAC-адреса динамического типа.

_____

_____

Убедитесь в том, что на коммутаторе S1 отключён доступ к VTY по Telnet. С помощью клиента Telnet, например Tera Term или PuTTY, попытайтесь посредством telnet подключиться к S1 с использованием адреса 192.168.1.11. Полученные результаты запишите ниже.

_____

С компьютера PC-A выполните проверку правильности работы SSH. Используя клиент SSH, например Tera Term или PuTTY, подключитесь посредством SSH к коммутатору S1 с компьютера PC-A. В случае получения сообщения с предупреждением об отличающемся ключе нажмите кнопку Continue («Продолжить»). Подключитесь с использованием соответствующего имени пользователя и пароля. Успешно ли был обработан эхо-запрос?

_____

Заполните идущую ниже таблицу сведениями о маршрутизаторе R1, используя для этого соответствующую команду или команды, применяемые на коммутаторе S1.

Идентификатор устройства	**Локальный интерфейс**	**Возможность настройки**	**Номер модели**	**Идентификатор удаленного порта**	**IP-адрес**	**Версия IOS**

a. Убедитесь в том, что все ваши пароли в файле конфигурации зашифрованы. Ниже запишите команду и полученные результаты.
   Команда:

   _____

   Пароль консоли зашифрован?

Шаг 3: Соберите сведения о компьютере PC-A.

С помощью различных команд служебных программ Windows вы сможете собрать сведения о PC-A.

a. В командной строке PC-A запустите на выполнение команду **ipconfig /all** и запишите ниже полученные результаты.

Укажите IP-адрес PC-A.

_____ Укажите маску подсети PC-A.

_____ Укажите адрес шлюза по умолчанию для PC-A.

_____ Укажите MAC-адрес компьютера PC-A.

_____

b. Выполните соответствующую команду для проверки связи стека протокола TCP/IP с сетевой интерфейсной платой. Какую команду вы использовали?

_____

c. Проверьте интерфейс закольцовывания маршрутизатора R1, выполнив команду Ping из командной строки компьютера PC-A. Успешно ли выполнен эхо-запрос?

_____

d. Выполните соответствующую команду на компьютере PC-A, чтобы получить список переходов по маршрутизаторам для пакетов, отправленных с PC-A на интерфейс закольцовывания маршрутизатора R1. Ниже запишите команду и полученный результат. Какую команду вы использовали?

_____

_____

e. Выполните соответствующую команду на компьютере PC-A, чтобы найти схему сопоставления адресов уровня 2 и уровня 3, используемую на вашей сетевой интерфейсной плате. Ниже запишите свои ответы. Запишите только ответы, относящиеся к сети 192.168.1.0/24. Какую команду вы использовали?

_____

Критерии оценивания практической работы

5 (отлично) – работа выполнена полностью и правильно, сделаны правильные выводы; работа выполнена по плану с учетом техники безопасности.

4 (хорошо) – работа выполнена правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – работа выполнена правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе работы, которые студент не может исправить даже по требованию преподавателя.

3.3 Фонд оценочных средств для рубежного контроля

Рубежный контроль проводится во время аудиторных занятий по ПМ

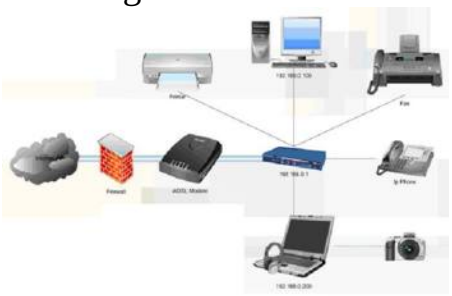
Эксплуатация объектов сетевой инфраструктуры в соответствии с учебным планом и рабочей программы ПМ.03 Эксплуатация объектов сетевой инфраструктуры.

Максимальное время выполнения задания: 40 мин.

Задача для решения определяется случайным образом по номеру журнала.

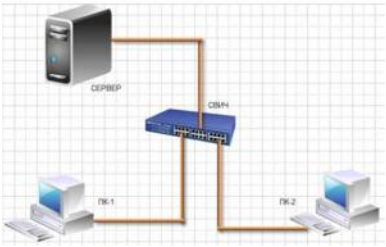
Вариант задания

1. Настройте сетевой интерфейс для введения компьютера в domain.
2. Настройте сетевую карту, имя компьютера, рабочую группу по заданным параметрам
3. Продемонстрируйте устранение неполадок с помощью PathPing
4. Продемонстрируйте устранение неполадок с помощью Ping
5. Продемонстрируйте устранение неполадок с использованием Network Diagnostics Framework
6. Выполните трассировку сети средствами утилиты Netsh
7. Сохраните кадры в текстовый файл.
8. Запишите данные средствами сетевого монитора
9. Выполните установку сетевого монитора
10. Используя оснастку Event Viewer, продемонстрируйте возможности работы с системными журналами.
11. Выполнить сканирование локальной сети с программой LanSurfer по заданным параметрам
12. Создайте профиль для сканирования Моё сканирование
13. Укажите диапазон адресов от 192.168.3.1 до 192.168.3.254
14. Просканируйте сеть
15. Используя возможности программы найдите файл MyTestXSetup.exe
16. Перейдите в папку содержащий данный файл.
17. Построить диаграмму сети с использованием программы EDraw Network Diagrammer



18. Построить диаграмму сети с использованием программы EDraw Network Diagrammer

19. Построить диаграмму сети с использованием программы EDraw Network Diagrammer



20. Построить схему сети с использованием программы 10-Strike LANState

21. Выполнить установку CommView Remote Agent и продемонстрировать возможности наблюдения трафика сети.

22. Выполнить настройку DNS Форвардера в WinRoute

23. Выполнить настройку DHCP-сервера в WinRoute

24. Выполнить базовую настройку политики трафика в WinRoute

25. Выполнить установку WinRoute

26. Создать группы BUH1 и BUH2 и распределить пользователей USER1 и USER12 по группам в domain соответственно.

27. Создать группы BUH1 и BUH2 средствами командной строки

28. Создать группы BUH1 и BUH2 в domain при помощи оснастки «Active Directory– пользователи и компьютеры»

29. Создать пароль для входа пользователю USER1 в domain

30. Создать пользователей средствами командной строки

31. Создать пользователя USER1 в domain на основании шаблонов.

32. Создать пользователя USER1 в domain при помощи оснастки «Active Directory– пользователи и компьютеры»

Критерии оценивания практической работы

5 (отлично) – задание выполнено полностью и правильно, сделаны правильные выводы; задание выполнено по плану с учетом техники безопасности.

4 (хорошо) – задание выполнено правильно с учетом 2-3 несущественных ошибок исправленных самостоятельно по требованию преподавателя.

3 (удовлетворительно) – задание выполнено правильно не менее чем на половину или допущена существенная ошибка.

2 (неудовлетворительно) – допущены две (и более) существенные ошибки в ходе задания, которые студент не может исправить даже по требованию преподавателя.

3.4 Фонд оценочных средств для промежуточной аттестации (экзамен)

На выполнение экзаменационной работы по ПМ дается 18 академических часов/ на диф.зачет по МДК выделяется 2 часа входящих в общее количество часов рабочей программы.

Экзамен по модулю предназначен для контроля и оценки результатов освоения профессионального модуля ПМ.03. Эксплуатация объектов сетевой инфраструктуры по специальности СПО 09.02.06. Сетевое и системное администрирование.

Экзамен квалификационный представляет собой ответы на два теоретические вопроса.

МДК.03.01. Безопасность компьютерных сетей

1. Принципы безопасности сетевого дизайна.
2. Безопасная архитектура.
3. Управление процессами и безопасность.
4. Тестирование сети на уязвимости.
5. Непрерывность бизнеса
6. Планирование восстановления аварийных ситуаций.
7. Жизненный цикл сети и планирование.
8. Разработка регламентов компании и политик безопасности.
9. VPN.
10. GRE VPN.
11. Компоненты и функционирование IPSec VPN.
12. Реализация Site-to-site IPSec VPN с использованием CLI.
13. Реализация Site-to-site IPSec VPN с использованием CCP.
14. Реализация Remote-access VPN.
15. Криптографические сервисы.
16. Базовая целостность и аутентичность.
17. Конфиденциальность.
18. Криптография открытых ключей
19. Обеспечение безопасности пользовательских компьютеров.
20. Соображения по безопасности второго уровня (Layer-2).
21. Конфигурация безопасности второго уровня.
22. Безопасность беспроводных сетей, VoIP и SAN.
23. IPS технологии.
24. IPS сигнатуры.
25. Реализация IPS.
26. Проверка и мониторинг IPS.
27. ACL.

28. Технология брандмауэра.
29. Контекстный контроль доступа (CBAC).
30. Политики брандмауэра основанные на зонах
31. Свойства AAA.
32. Локальная AAA аутентификация.
33. Server-based AAA
34. Современные угрозы сетевой безопасности.
35. Вирусы, черви и троянские кони.
36. Методы атак

МДК.03.02. Эксплуатация объектов сетевой инфраструктуры

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. Добавление отдельных элементов сети (пользователей, компьютеров, приложений, служб).
5. Наращивание длины сегментов сети; замена существующей аппаратуры.
6. Увеличение количества узлов сети; увеличение протяженности связей между объектами сети.
7. Техническая и проектная документация.
8. 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. Оборудование для диагностики и сертификации кабельных систем.
18. Сетевые мониторы, приборы для сертификации кабельных систем, кабельные сканеры и тестеры.

19. Настройка H.323. Описание H.323 и общие рекомендации. Функциональные компоненты H.323.Установка и поддержка соединения H.323. Соединения без и с использованием GateKeeper. Соединения с использованием нескольких GateKeeper.

20. Многопользовательские конференции. Обеспечение отказоустойчивости.

21. Настройка SIP. Описание и общие рекомендации. Технология SIP и связанные с ней стандарты. Функциональные компоненты SIP. Сообщения SIP. Адресация SIP.

22. Модель установления соединения. Планирование отказоустойчивости.

23. Установка и инсталляция программного коммутатора.

24. Монтажные процедуры.

25. Процедуры инсталляции.

26. Управление аппаратными средствами и портами. Протоколы управления MGCP, H.248. Создание аналоговых абонентов.

27. Внутристанционная маршрутизация.

28. Управление программным коммутатором. Маршрутизация. Группы соединительных линий.

29. Подключение станций с TDM (абонентский доступ TDM). Сигнализация SIP, SIP-T, H.323 и SIGTRAN. IP-абоненты. Группы абонентов. Дополнительные абонентские услуги.

30. Организация эксплуатации систем IP-телефонии.

31. Техническое обслуживание, плановый текущий ремонт, плановый капитальный ремонт, внеплановый ремонт.

32. Восстановление работы сети после аварии.

33. Схемы послеаварийного восстановления работоспособности сети, техническая и проектная документация, способы резервного копирования данных, принципы работы хранилищ данных;

Из данных вопросов формируется 30 билетов, время подготовки студентов 45 минут.

Критерии оценки экзамена

5 «отлично» выставляется, если студент:

- полностью раскрыл содержание материала в объеме, предусмотренном программой и учебником, правильно решил практическое задание;
- изложил материал грамотным языком в определенной логической последовательности, точно используя математическую и специализированную терминологию и символику;
- правильно выполнил практическое задание, сопутствующие ответу;

- показал умение иллюстрировать теоретические положения конкретными примерами, применять их в новой ситуации при выполнении практического задания;
- продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;
- отвечал самостоятельно без наводящих вопросов преподавателя (возможны одна-две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя).

4 «хорошо» выставляется, если:

ответ удовлетворяет в основном требованиям на оценку «5», но при этом имеет один из недостатков:

- в изложении допущены небольшие пробелы, не исказившие логического и информационного содержания ответа;
- допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя;
- допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.

3 «удовлетворительно» выставляется, если:

- неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, практике и выкладках, исправленные после нескольких наводящих вопросов преподавателя;
- студент не справился с применением теории в новой ситуации при выполнении практического задания, но выполнил задания обязательного уровня сложности по данной теме;
- при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

2 «неудовлетворительно» выставляется, если:

- не раскрыто основное содержание учебного материала;
- обнаружено незнание или непонимание студентом большей или наиболее важной части учебного материала;
- допущены ошибки в определении понятий, при использовании терминологии, в чертежах, блок-схем и иных выкладках, которые не исправлены после нескольких наводящих вопросов преподавателя;
- студент обнаружил полное незнание и непонимание изучаемого учебного материала или не смог ответить ни на один из поставленных вопросов по изучаемому материалу.

Процент результативности	Качественная оценка индивидуальных образовательных

	достижений	
	балл (отметка)	вербальный аналог
90-100	5	отлично
80-89	4	хорошо
70-79	3	удовлетворительно
менее 70	2	не удовлетворительно

4.Список литературы

1. Назаров, А. В. Эксплуатация объектов сетевой инфраструктуры : учебник / А.В. Назаров, А.Н. Енгалычев, В.П. Мельников. - Москва : КУРС ; ИНФРА-М, 2017. — 360 с.

2. Руденков, Н.А.. Технологии защиты информации в компьютерных сетях: Курс лекций / Н.А. Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов — Москва : Интуит НОУ, 2019. — 368 с. — URL: https://book.ru/book/918258— Текст : электронный. (book.ru)