

МИНОБРНАУКИ РОССИИ
ВЛАДИВОСТОКСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

**РАБОЧАЯ ПРОГРАММА
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

ПМ.02 Организация сетевого администрирования

программы подготовки специалистов среднего звена
09.02.06 Сетевое и системное администрирование

Форма обучения: очная

Владивосток 2024

СОДЕРЖАНИЕ

- 1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 2. СТРУКТУРА И СОДЕРЖАНИЕ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**
- 3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО
МОДУЛЯ**
- 4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ
ПРОФЕССИОНАЛЬНОГО МОДУЛЯ**

Рабочая программа ПМ.02 Организация сетевого администрирования разработана в соответствии с требованиями Федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минобрнауки России от 10.07.2023, №519, примерной образовательной программой.

Разработчик(и): Е.А. Стефанович, преподаватель

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № 10 от « 16 » 05 2024 г.

Председатель ЦМК  Е.А. Стефанович
подпись

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ «ПМ.02 ОРГАНИЗАЦИЯ СЕТЕВОГО АДМИНИСТРИРОВАНИЯ ОПЕРАЦИОННЫХ СИСТЕМ»

1.1. Цель и планируемые результаты освоения профессионального модуля

В результате изучения профессионального модуля обучающийся должен освоить основной вид деятельности «Организация сетевого администрирования операционных систем» и соответствующие ему общие компетенции и профессиональные компетенции:

1.1.1. Перечень общих компетенций

| Код | Наименование общих компетенций |
|--------|---|
| ОК 01. | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам |
| ОК 02. | Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам |
| ОК 03. | Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по финансовой грамотности в различных жизненных ситуациях. |

1.1.2. Перечень профессиональных компетенций

| Код | Наименование видов деятельности и профессиональных компетенций |
|--------|---|
| ВД 2. | Организация сетевого администрирования операционных систем |
| ПК 2.1 | Принимать меры по устранению сбоев |
| ПК 2.2 | Администрировать сетевые ресурсы в операционных системах |
| ПК 2.3 | Осуществлять сбор данных для анализа использования и функционирования программно-технических средств компьютерных сетей |
| ПК 2.4 | Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения |
| ПК 2.5 | Осуществлять выявление и устранение инцидентов в процессе функционирования операционных систем |

1.1.3. В результате освоения профессионального модуля обучающийся должен

| | |
|--|---|
| Владеть навыками | выявления и определения сбоев и отказов сетевых устройств, и операционных систем; |
| | устранения последствий сбоев и отказов сетевых устройств и операционных систем; |
| | регистрации сообщений об ошибках в сетевых устройствах и операционных системах; |
| | обнаружения критических инцидентов и причин возникновения критических инцидентов при работе прикладного программного обеспечения; |
| | выполнения действий по устранению критических инцидентов при работе прикладного программного обеспечения в рамках должностных обязанностей; |
| | идентификации инцидентов при работе прикладного программного обеспечения. |
| | сопоставления аварийной информации от различных устройств информационно-коммуникационной системы; |
| | локализации отказов в сетевых устройствах и операционных системах; |
| | контроля ежедневных отчетов от систем мониторинга и системы сбора и передачи учетной информации; |
| исправления ошибок конфигурации сетевых устройств и операционных систем; | |

| | |
|-------|---|
| | составления отчетов об использовании сетевых ресурсов и операционных системах. |
| | восстановления параметров по умолчанию согласно документации операционных систем; |
| | восстановления параметров при помощи серверов архивирования и средств управления специализированных операционных систем сетевого оборудования; |
| | мониторинга проведенного планового архивирования пользовательских устройств |
| | запуска, мониторинга и контроля процедуры установки прикладного программного обеспечения на конечных устройствах пользователей и/или серверном оборудовании |
| | резервного копирования программного обеспечения технических средств |
| | работы с системой по контролю за профилактическим обслуживанием |
| | выполнения обновления программного обеспечения технических средств согласно инструкции |
| | подготовки к проведению предварительных испытаний |
| | выполнения резервного копирования программного обеспечения технических средств, попадающих в область потенциального домена возникновения сбоя |
| | возврата информационно-коммуникационной системы к первоначальному состоянию после окончания предварительных испытаний |
| Уметь | идентифицировать и оценивать степень критичности инцидентов, возникающих при установке и работе программного обеспечения, и принимать решение по изменению процедуры установки; |
| | устранять возникающие инциденты; |
| | локализовать отказ и инициировать корректирующие действия; |
| | пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; |
| | выполнять мониторинг администрируемой информационно-коммуникационной системы; |
| | конфигурировать операционные системы сетевых устройств |
| | использовать современные методы контроля производительности информационно-коммуникационной систем; |
| | локализовать отказ и инициировать корректирующие действия; |
| | применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; |
| | применять внешние и штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы. |
| | использовать процедуры восстановления данных; |
| | определять точки восстановления данных; |
| | работать с серверами архивирования и средствами управления операционных систем; |
| | пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; |
| | выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику. |
| | соблюдать процедуру установки прикладного программного обеспечения в соответствии с требованиями организации- производителя |
| | идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение по изменению процедуры установки |
| | пользоваться нормативно-технической документацией в области инфокоммуникационных технологий |
| | использовать различные средства и режимы установки и обновления программного обеспечения информационно-коммуникационной системы, в том числе автоматические |

| | |
|-------|---|
| | идентифицировать инциденты, возникающие при проведении предварительных испытаний |
| | использовать процедуры восстановления данных |
| | определять точки восстановления данных |
| | оценивать риски перерывов в предоставлении сервисов при проведении испытаний |
| | применять нормативно-техническую документацию в области инфокоммуникационных технологий |
| Знать | лицензионных требований по настройке и эксплуатации устанавливаемого программного обеспечения; |
| | основ архитектуры, устройства и функционирования вычислительных систем; |
| | принципов организации, состава и схем работы операционных систем; |
| | требований охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы. |
| | принципов организации, состава и схем работы операционных систем; |
| | требований охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы. |
| | лицензионных требований по настройке и эксплуатации |
| | принципов организации инфокоммуникационных систем по управлению ремонтом и обслуживанием; |
| | типовых сроков проведения профилактических ремонтов; |
| | терминологии и правил чтения технической документации; |
| | правил оформления технической документации по результатам проверки работоспособности устройств инфокоммуникационных систем. |
| | основ архитектуры аппаратных средств; |
| | принципов функционирования аппаратных средств вычислительной техники; |
| | типовых регламентов обслуживания аппаратных средств; |
| | способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; |
| | требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем. |
| | лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; |
| | основы архитектуры, устройства и функционирования вычислительных систем; |
| | требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы. |
| | общих принципов функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; |
| | международных стандартов локальных вычислительных сетей; |
| | регламентов проведения профилактических работ на администрируемой информационно-коммуникационной системе; |
| | требований охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системе |
| | лицензионные требования по настройке устанавливаемого программного обеспечения |
| | типовые причины инцидентов, возникающих при установке программного обеспечения |
| | требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой инфокоммуникационной системы |

| | |
|--|---|
| | типовые процедуры и стандарты обновления программного обеспечения технических средств |
| | лицензионные требования по настройке обновляемого программного обеспечения |
| | принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети |
| | архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы |
| | регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе |
| | требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы |

1.2. Количество часов, отводимое на освоение профессионального модуля

Всего часов 567

в том числе в форме практической подготовки 431

Из них на освоение МДК 309

в том числе самостоятельная работа 65

практики, в том числе учебная 108

производственная 144

Промежуточная аттестация 18

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

2.1. Структура профессионального модуля

| Коды профессиональных и общих компетенций | Наименования разделов профессионального модуля | Всего, час. | В т.ч. в форме практической подготовки | Объем профессионального модуля, ак. час. | | | | | | |
|---|---|-------------|--|--|-------------------------------------|---------------------------|------------------------|--------------------------|----------|------------------|
| | | | | Обучение по МДК | | | | | Практики | |
| | | | | Всего | В том числе | | | | Учебная | Производственная |
| | | | | | Лабораторных и практических занятий | Курсовых работ (проектов) | Самостоятельная работа | Промежуточная аттестация | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| ПК 2.1-2.5 ОК 01-03 | Раздел 1. Администрирование сетевых операционных систем | 88 | 54 | 86 | 64 | | 18 | 4 | | |
| ПК 2.1-2.5 ОК 01-03 | Раздел 2. Программное обеспечение компьютерных сетей | 83 | 51 | 81 | 60 | | 17 | 4 | | |
| ПК 2.1-2.5 ОК 01-03 | Раздел 3. Организация администрирования компьютерных систем | 138 | 104 | 136 | 84 | | 18 | 30 | | |
| | Учебная практика | 108 | 108 | | | | | | 108 | |
| | Производственная практика | 144 | 144 | | | | | | | 144 |
| | Экзамен по модулю | | | | | | | 6 | | |
| | Всего: | 561 | 431 | 303 | 208 | 18 | | 12 | 108 | 144 |

1.2. Тематический план и содержание профессионального модуля (ПМ)

| Наименование разделов и тем профессионального модуля (ПМ), междисциплинарных курсов (МДК) | Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная учебная работа обучающихся, курсовая работа (проект) | Объем, акад. ч / в том числе в форме практической подготовки, акад. ч ¹ | Коды компетенций, формированию которых способствует элемент программы |
|---|---|--|---|
| Раздел 1. Администрирование сетевых операционных систем | | 88/54 | |
| МДК.02.01. Администрирование сетевых операционных систем | | 88/54 | |
| Тема 1.1. Администрирование Linux | <p>Содержание</p> <p>1. Введение Введение в дисциплину. Знакомство с системой виртуализации.</p> <p>2. Файловые системы ОС Linux Файловые системы ОС Linux. Создание и разметка жесткого диска</p> <p>3. Подготовка сервера ОС Linux Варианты установки. Резервное копирование. Создание снимков. Разметка жесткого диска.</p> <p>4. Настройка сервера DHCP в ОС Linux Протокол DHCP</p> <p>5. Настройка сервера DNS в ОС Linux Протокол DNS</p> <p>6. Настройка web-серверов в ОС Linux Протокол HTTP. Веб-сервер Nginx. Обратное проксирование в Nginx.</p> <p>7. Настройка файловых серверов в ОС Linux Протокол FTP. Файловая система NFS. Файловый сервер Samba.</p> <p>8. Настройка серверов БД в ОС Linux СУБД MariaDB. СУБД Postgres</p> <p>9. Контейнеры Docker Контейнеры Docker. Способы связи контейнеров Docker.</p> | 32 | ПК 2.1-2.5 ОК 01-03 |

¹ Распределение по темам осуществляется разработчиками рабочей программы самостоятельно.

| | | | |
|---|---|--------------|------------------------|
| | В том числе практических занятий и лабораторных работ | 32 | |
| | Практическое занятие 1. Установка и базовая настройка ОС Linux. | 7 | |
| | Практическое занятие 2. Знакомство с основными командами, правами доступа и файловой системой | 7 | |
| | Практическое занятие 3. Установка DHCP сервера. Настройка DHCP сервера. Поиск и устранение неисправностей конфигурации. | 6 | |
| | Практическое занятие 4. Установка DNS сервера. Настройка DHCP сервера. Поиск и устранение неисправностей конфигурации. | 6 | |
| | Практическое занятие 5. Создание Docker контейнеров с различными сервисами. Отладка сервисов. Обеспечение сетевой связности группы контейнеров. | 6 | |
| Раздел 2. Программное обеспечение компьютерных сетей | | 83/51 | |
| МДК.02.02. Программное обеспечение компьютерных сетей | | 83/51 | |
| Тема 2.1. Программные средства мониторинга компьютерных сетей | Содержание | | |
| | 1. Введение в системы мониторинга Виды мониторинга (агентный, безагентный, аналитический). Программные средства для сбора анализа и обработки данных | 30 | ПК 2.1-2.5 ОК 01-03 |
| | 2. Wireshark как система мониторинга Особенности, установка, настройка. Захват, анализ и интерпретация сетевого трафика. | | |
| | 3. Система мониторинга Zabbix Особенности, установка, настройка. Понятие агентов. Понятие шаблонов. Понятие триггеров. Интеграция с внешними приложениями. Анализ и отчеты | | |
| | 4. Введение в систему мониторинга Nagios, обзор основных функций и особенностей Установка и базовая настройка сервера. Создание и настройка уведомлений. Использование плагинов и их настройка. Интеграция Nagios с другими системами мониторинга | | |
| | В том числе практических занятий и лабораторных работ | 30 | |
| | Практическое занятие 1. Настройка Wireshark. Захват и анализ сетевого трафика с помощью Wireshark. Интерпретация полученных результатов мониторинга. | 10 | |
| Практическое занятие 2. Установка и настройка Zabbix. Работа с агентами и шаблонами. Настройка триггеров для мониторинга производительности и доступности приложений и сервисов. Интеграция Zabbix с внешними приложениями. Создание отчетов и анализ результатов мониторинга | 10 | | |

| | | | |
|---|---|----------------|------------------------|
| | Практическое занятие 3. Установка и базовая настройка сервера Nagios. Создание и настройка уведомлений при возникновении проблем. Использование плагинов и настройка их работы. Интеграция Nagios с другими системами мониторинга для расширения функциональности | 10 | |
| Раздел 3. Организация администрирования компьютерных систем | | 138/104 | |
| МДК.02.03. Организация администрирования компьютерных систем | | 138/104 | |
| Тема 3.1. Технологии контейнеризации | Содержание | | |
| | 1. Введение в контейнеризацию Основные понятия и принципы работы. Тенденции развития технологий контейнеризации | 32 | ПК 2.1-2.5 ОК 01-03 |
| | 2. Сравнение Docker с другими технологиями контейнеризации runc, Podman, Scoreo | | |
| | 3. Архитектура Docker Образы. Контейнеры. Docker-registry. Docker Desktop | | |
| | 4. Создания образов Docker с использованием Dockerfile Синтаксис. Основные команды | | |
| | 5. Docker-compose Язык разметки YAML. Развертывание окружения из нескольких контейнеров | | |
| | 6. Расширенная настройка Docker-compose Взаимодействие с файловой системой. Docker-network. Управление портами контейнеров. Переменные окружения | | |
| | 7. Введение в Kubernetes Основные понятия и принципы работы. Тенденции развития Kubernetes | | |
| | 8. Архитектура Kubernetes Компоненты и их взаимодействие. Мастер-ноды. API-сервер Kubernetes. Репликация компонентов | | |
| | 9. Кластеры Kubernetes Установка, настройка и масштабирование кластера. Управление ресурсами в Kubernetes кластере. Использование Service и Ingress | | |
| | 10. Хранилища данных Kubernetes Описание и основные концепции. Persistent Volumes и Persistent Volume Claims. Резервное копирование и восстановление данных | | |
| 11. Управление сетями кластера Kubernetes Конфигурация сетевых политик в Kubernetes. Управление DNS в Kubernetes. Контроль доступа в сетях Kubernetes. Маршрутизация трафика в Kubernetes | | | |

| | | | |
|--|---|-----------|--|
| | В том числе практических занятий и лабораторных работ | 52 | |
| | Практическое занятие 1. Создание и запуск образа Docker | 7 | |
| | Практическое занятие 2. Работа с Docker Hub и локальным реестром | 6 | |
| | Практическое занятие 3. Использование Docker-compose для развёртывания многоконтейнерного окружения | 7 | |
| | Практическое занятие 4. Создание собственных сетей в Docker и настройка взаимодействия между контейнерами | 6 | |
| | Практическое занятие 5. Работа с файловой системой контейнера и управление внешними файлами и директориями. Использование переменных окружения в контейнерах Docker | 7 | |
| | Практическое занятие 6. Установка и настройка локального Kubernetes кластера с помощью Minikube | 6 | |
| | Практическое занятие 7. Создание и масштабирование подов в Kubernetes кластере | 7 | |
| | Практическое занятие 8. Работа с Kubernetes Service для обеспечения доступа к приложению извне | 6 | |
| Учебная практика | | | |
| Виды работ | | | |
| <ol style="list-style-type: none"> 1. Администрирование серверов и рабочих станций; 2. Организация доступа к локальным сетям и Интернету; 3. Установка и сопровождение сетевых сервисов; 4. Расчёт стоимости сетевого оборудования и программного обеспечения; 5. Сбор данных для анализа использования программно-технических средств компьютерных сетей; 6. Обеспечение сетевой безопасности. | | 108 | |
| Производственная практика | | | |
| Виды работ | | | |
| <ol style="list-style-type: none"> 1. Установка на серверы и рабочие станции: операционные системы и необходимое для работы программное обеспечение; 2. Поддержка в работоспособном состоянии программное обеспечение серверов и рабочих станций; 3. Регистрация пользователей локальной сети и почтового сервера, назначает идентификаторы и пароли; 4. Обеспечение своевременного копирования, архивирования и резервирования данных; 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; | | 144 | |

| | | |
|---|----|--|
| <ol style="list-style-type: none"> 6. Проведение мониторинга сети, разрабатывать предложения по развитию инфраструктуры сети; 7. Обеспечение сетевой безопасности (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных), безопасность межсетевого взаимодействия; 8. Осуществление антивирусной защиты локальной вычислительной сети, серверов и рабочих станций; 9. Документирование всех произведенных действий. | | |
| <p>Курсовой проект (работа) Обучающийся имеет право выбора: выполнять курсовой проект по тематике данного или иного профессионального модуля(ей) или общепрофессиональной дисциплине(-ам).</p> <p>Тематика курсовых проектов (работ)</p> <ol style="list-style-type: none"> 1. Сравнительный анализ гипервизоров: VMware ESXi, Microsoft Hyper-V и KVM; 2. Контейнеризация или виртуализация: Преимущества и недостатки для бизнеса; 3. Оптимизация производительности виртуальных машин в среде VMware vSphere; 4. Автоматизация развертывания и управления контейнерами с использованием Kubernetes; 5. Безопасность контейнерных сред: Лучшие практики и инструменты; 6. Развертывание и управление виртуальными сетями с использованием Microsoft Hyper-V; 7. Использование Docker для создания изолированных сред разработки и тестирования; 8. Автоматизация развертывания и управления контейнерами с использованием Docker-compose; 9. Виртуализация рабочих столов (VDI): Технологии, преимущества и реализация. | | |
| <p>Обязательные аудиторные учебные занятия по курсовому проекту (работе)</p> <ol style="list-style-type: none"> 1. Обзор основных понятий, задач и инструментов, необходимых для администрирования компьютерных систем (Лекция с использованием презентационных материалов и реальных примеров); 2. Рассмотрение критериев выбора гипервизоров для корпоративной инфраструктуры (Дискуссия и анализ существующих решений на рынке); 3. Основы создания и настройки виртуальных машин на платформе VMware vSphere или Microsoft Hyper-V (Практическое занятие в компьютерном классе с использованием соответствующего программного обеспечения); 4. Основы работы с Docker, создание контейнеров и управление ими (Практическое занятие с демонстрацией и выполнением заданий); 5. Основы виртуализации рабочих столов (VDI) Практическое занятие с демонстрацией и выполнением заданий); 6. Рассмотрение критериев реализации безопасности контейнерных сред (Дискуссия и анализ лучших практик и инструментов в профессии). | 18 | |

| | | |
|--|-------------------|--|
| <p>Самостоятельная учебная работа обучающегося над курсовым проектом (работой)</p> <ol style="list-style-type: none"> 1. Планирование выполнения курсового проекта (работы); 2. Определение задач работы; 3. Изучение литературных источников; 4. Проведение предпроектного исследования; 5. Проектирование компьютерной сети медицинского центра с несколькими филиалами; 6. Разработка системы мониторинга и управления IT-инфраструктурой производственного предприятия; 7. Проектирование беспроводной сети Wi-Fi для торгового центра; 8. Создание отказоустойчивой системы хранения данных для банка; 9. Проектирование системы видеонаблюдения и контроля доступа для офисного здания; 10. Разработка системы резервного копирования и восстановления данных для IT-компании; 11. Проектирование сети VoIP-телефонии для call-центра; 12. Создание системы виртуализации серверов для хостинг-провайдера; 13. Проектирование системы информационной безопасности для государственной организации; 14. Разработка системы управления IT-активами и лицензиями для крупной корпорации; 15. Создание системы автоматизированного развертывания и управления конфигурациями серверов; 16. Проектирование сети хранения данных (SAN) для дата-центра; 17. Разработка системы мониторинга производительности приложений и серверов для интернет-магазина; 18. Проектирование программно-определяемой сети (SDN) для провайдера телекоммуникационных услуг; 19. Создание системы единого входа (SSO) для корпоративных web-приложений; 20. Проектирование отказоустойчивого кластера серверов баз данных для социальной сети; 21. Разработка системы защиты от DDoS-атак для новостного интернет-портала; 22. Проектирование системы удаленного доступа и VPN для распределенной компании; 23. Разработка системы управления инцидентами и проблемами для IT-службы предприятия; 24. Проектирование катастрофоустойчивой инфраструктуры для банка; 25. Создание системы контейнеризации приложений для DevOps-команды. | | |
| <p>Всего</p> | <p>478</p> | |

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

3.1. Для реализации программы профессионального модуля должны быть предусмотрены следующие специальные помещения:

Лаборатория «Сетевого администрирования операционных систем», оснащенная в соответствии с п. 6.1.2.3 образовательной программы по специальности.

Оснащенные базы практики, в соответствии с п. 6.2.1.5 образовательной программы по специальности.

3.2. Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд образовательной организации должен иметь печатные и/или электронные образовательные и информационные ресурсы для использования в образовательном процессе. При формировании библиотечного фонда образовательной организации выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список может быть дополнен новыми изданиями.

3.2.1. Основные печатные и электронные издания

26. Организация сетевого администрирования : учебник / А.И. Баранчиков, П.А. Баранчиков, А.Ю. Громов, О.А. Ломтева. — Москва : КУРС : ИНФРА-М, 2023. — 384 с. - ISBN 978-5-906818-34-8. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1912998> (дата обращения: 02.09.2023). – Режим доступа: по подписке.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОФЕССИОНАЛЬНОГО МОДУЛЯ

| 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. 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. Осуществлять проведение обновления программного обеспечения операционных систем и прикладного программного обеспечения ПК.2.5. Осуществлять выявление и устранение инцидентов в процессе | 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. Демонстрирует освоение общих | Зачет в форме собеседования: практическое задание по построению алгоритма в соответствии с техническим заданием Защита отчетов по практическим и лабораторным работам Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы Экспертное наблюдение и оценка на лабораторно - |

| | | |
|---|---|---|
| <p>функционирования операционных систем</p> <p>ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.</p> <p>ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.</p> <p>ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие</p> | <p>компетенций при решении профессиональных задач</p> | <p>практических занятиях, при выполнении работ по учебной и производственной практикам</p> <p>Экзамен по модулю</p> |
|---|---|---|

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Владивостокский государственный университет»
Колледж сервиса и дизайна

КОНТРОЛЬНО-ОЦЕНОЧНЫЕ СРЕДСТВА
для проведения текущего контроля и промежуточной аттестации
Профессионального модуля
ПМ.02 Организация сетевого администрирования
программы подготовки специалистов среднего звена /
квалифицированных рабочих и служащих
09.02.06 «Сетевое и системное администрирование»

Форма обучения: очная

Владивосток 2024

Контрольно-оценочные средства для проведения текущего контроля и промежуточной аттестации по профессиональному модулю ПМ.02 «Организация сетевого администрирования» разработаны в соответствии с требованиями ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, утвержденного приказом Минобрнауки РФ от 09.12.2016, №1548.

Разработчик(и):

Коротков П.К., преподаватель колледжа сервиса и дизайна ВВГУ;
Головин Д.И., преподаватель колледжа сервиса и дизайна ВВГУ.

Рассмотрено и одобрено на заседании цикловой методической комиссии

Протокол № ___ от « ___ » _____ 20 ___ г.

Председатель ЦМК _____ Е.А. Стефанович
подпись

1 Общие сведения

Контрольно-оценочные средства (далее – КОС) предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу профессионального модуля ПМ.02 Организация сетевого администрирования.

КОС включают в себя контрольные материалы для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине, которая проводится в форме дифференцированного зачёта (с использованием оценочного средства – устный опрос в форме ответов на вопросы, устный опрос в форме собеседования, выполнение письменных заданий, тестирование и т.д.)

2 Планируемые результаты обучения по профессиональному модулю, обеспечивающие результаты освоения образовательной программы

| Код ОК, ПК ¹ | Код результата обучения ¹ | Наименование результата обучения ¹ |
|-----------------------------|--|--|
| ОК 01-3 ПК 2.1-2.5 | ПО1 | Практический опыт настройки сетевых устройств |
| | ПО2 | Практический опыт настройки и поддержания серверных систем |
| | ПО3 | Практический опыт в обеспечении бесперебойной работы сети |
| | ПО4 | Практический опыт администрирования систем управления сетью |
| | 31 | Знание основных функций и компоненты Windows Server 2012 R2 |
| | 32 | Знание базовых принципов установки и настройки серверной операционной системы |
| | 33 | Знание процессов резервного копирования и восстановления данных на сервере |
| | 34 | Знание методов мониторинга и диагностики состояния сервера |
| | 35 | Знание основных команд и концепций командной строки Linux |
| | 36 | Способность изложить современные сетевые технологии, в том числе протоколы, стандарты и топологии. |
| | 37 | Способность изложить методы взаимодействия настольных приложений с сетевой инфраструктурой |
| | 38 | Способность изложить методы обеспечения безопасности и защиты данных при работе с настольными приложениями |
| | 39 | Способность понимать архитектуру сетевых серверов Cisco и их конфигурации. |
| | 310 | Способность перечислить методы обеспечения высокой доступности, таких как кластеризация и резервирование, с использованием Linux-серверов и оборудования Cisco. |
| | У1 | Умение проводить установку Windows Server 2012 R2 на физическое или виртуальное оборудование |
| | У2 | Умение настраивать и управлять службами сетевых протоколов, такими как DNS, DHCP и другими |
| | У3 | Умение решать типичные задачи, связанные с администрированием Linux, такие как настройка прав доступа, настройка сети, установка и обновление программного обеспечения |
| У4 | Умение диагностировать и устранять проблемы, возникающие на серверах и рабочих станциях Linux | |
| У5 | Способность решать типичные задачи и проблемы, связанные с клиентской инфраструктурой, такие как настройка сетевых параметров, диагностика и устранение сетевых проблем. | |

| Код ОК, ПК ¹ | Код результата обучения ¹ | Наименование результата обучения ¹ |
|-------------------------|--------------------------------------|--|
| | У6 | Способность анализировать и оптимизировать сетевую инфраструктуру в соответствии с требованиями организации. |
| | У7 | Способность устанавливать, настраивать и управлять групповой политикой для клиентских систем и настольных приложений. |
| | У8 | Способность настраивать и управлять сетевыми устройствами Cisco, включая маршрутизаторы и коммутаторы. |
| | У9 | Способность диагностировать и устранять проблемы в работе серверов и сетевого оборудования Cisco, включая быстрое восстановление после сбоев. |
| | У10 | Способность решать типичные задачи и проблемы, связанные с клиентской инфраструктурой, такие как настройка сетевых параметров, диагностика и устранение сетевых проблем. |

¹- в соответствии с рабочей программой профессионального модуля

3 Соответствие оценочных средств контролируемым результатам обучения
Средства, применяемые для оценки уровня теоретической и практической
подготовки

| Краткое наименование раздела (модуля) / темы дисциплины | Код результата обучения | Показатель ² овладения результатами обучения | Наименование оценочного средства и представление его в КОС ³ | |
|---|-------------------------|--|---|---------------------------------------|
| | | | Текущий контроль ⁴ | Промежуточная аттестация ⁴ |
| Раздел 1. Администрирование сетевых операционных систем / МДК.02.01. Администрирования сетевых операционных систем | | | | |
| Тема 1.1 Установка и настройка Windows Server 2012 R2 | 31 | Способность перечислить основные функции и компоненты Windows Server 2012 R2. | Конспект лекций, Устный опрос (п. 5.1, вопросы 1-10) | Вопросы на экзамен 1-6 (п. 6.1) |
| | 32 | Способность изложить базовые принципы установки и настройки серверной операционной системы. | Конспект лекций, Устный опрос (п. 5.1, вопросы 11-20) | Вопросы на экзамен 7-12 (п. 6.1) |
| | У1 | Способность проводить установку Windows Server 2012 R2 на физическое или виртуальное оборудование. | Конспект лекций, Тест № 1 (п.5.2, варианты 1-3) | Лабораторная работа № 1 |
| Тема 1.2 Администрирование Windows Server 2012 R2 | 33 | Способность понимать процессы резервного копирования и восстановления данных на сервере. | Конспект лекций, Контрольная работа № 1 (п.5.4, задания 1-10) | Лабораторная работа № 2 |
| | 34 | Способность перечислить методы мониторинга и диагностики состояния сервера. | Конспект лекций, Контрольная работа № 2 (п.5.4, задания 1-10) | Лабораторная работа № 3-4 |
| | У2 | Способность настраивать и управлять службами сетевых протоколов, такими как DNS, DHCP и другими. | Конспект лекций, Практическое задание № 1 | Тест № 1 (п.6.2) |
| Тема 1.3 Основы Linux | 35 | Способность перечислить основные команды и концепции командной строки Linux. | Конспект лекций, Доклад (п.5.5, темы 1-10) | Вопросы на экзамен 13-18 (п. 6.1) |
| | У3 | Способность решать типичные задачи, связанные с администрированием Linux, такие как настройка прав доступа, настройка сети, установка и обновление | Конспект лекций, Тест № 2 (п.5.2) | Вопросы на экзамен 19-24 (п. 6.1) |

| Краткое наименование раздела (модуля) / темы дисциплины | Код результата обучения | Показатель ² овладения результатами обучения | Наименование оценочного средства и представление его в КОС ³ | |
|---|-------------------------|--|---|---------------------------------------|
| | | | Текущий контроль ⁴ | Промежуточная аттестация ⁴ |
| | | программного обеспечения. | | |
| | У4 | Способность диагностировать и устранять проблемы, возникающие на серверах и рабочих станциях Linux. | Конспект лекций, Практическое задание № 2 | Тест № 2 (п.6.2) |
| Раздел 2. Программное обеспечение компьютерных сетей | | | | |
| МДК.02.02. Программное обеспечение компьютерных сетей | | | | |
| Тема 2.1. Реализация клиентской инфраструктуры | 36 | Способность изложить современные сетевые технологии, в том числе протоколы, стандарты и топологии. | Конспект лекций, Доклад (п.5.5, темы 11-20) | Вопросы на экзамен 25-30 (п. 6.1) |
| | У5 | Способность решать типичные задачи и проблемы, связанные с клиентской инфраструктурой, такие как настройка сетевых параметров, диагностика и устранение сетевых проблем. | Конспект лекций, Тест № 3 (п.5.2, варианты 1-2) | Лабораторная работа № 5 |
| | У6 | Способность анализировать и оптимизировать сетевую инфраструктуру в соответствии с требованиями организации. | Конспект лекций, Практическое задание № 3 | Тест № 3 (п.6.2) |
| Тема 2.2. Реализация среды настольных приложений | 37 | Способность изложить методы взаимодействия настольных приложений с сетевой инфраструктурой | Конспект лекций, Доклад (п.5.5, темы 21-30) | Вопросы на экзамен 31-36 (п. 6.1) |
| | 38 | Способность изложить методы обеспечения безопасности и защиты данных при работе с настольными приложениями | Конспект лекций, Доклад (п.5.5, темы 31-40) | Вопросы на экзамен 37-42 (п. 6.1) |
| | У7 | Способность устанавливать, настраивать и управлять групповой политикой для клиентских систем и настольных приложений. | Конспект лекций, Контрольная работа № 3 (п.5.4, задания 1-10) | Лабораторная работа № 6 |
| Раздел 3. Организация администрирования компьютерных систем | | | | |
| МДК 02.03. Организация администрирования компьютерных систем | | | | |
| Тема 3.1 Проектирование и реализация серверной инфраструктуры | 39 | Способность понимать архитектуру сетевых серверов Cisco и их конфигурации. | Конспект лекций, Доклад (п.5.5, темы 21-30) | Вопросы на экзамен 43-48 (п. 6.1) |
| | У8 | Способность настраивать и управлять сетевыми | Конспект лекций, | Лабораторная работа № 7 |

| Краткое наименование раздела (модуля) / темы дисциплины | Код результата обучения | Показатель ² овладения результатами обучения | Наименование оценочного средства и представление его в КОС ³ | |
|---|-------------------------|---|---|---------------------------------------|
| | | | Текущий контроль ⁴ | Промежуточная аттестация ⁴ |
| ры | | устройствами Cisco, включая маршрутизаторы и коммутаторы. | Устный опрос (п. 5.1, вопросы 21-30) | |
| Тема 3.2. Реализация продвинутой серверной инфраструктуры | 310 | Способность перечислить методы обеспечения высокой доступности, таких как кластеризация и резервирование, с использованием Linux-серверов и оборудования Cisco. | Конспект лекций, Контрольная работа № 4 (п.5.4, задания 1-10) | Вопросы на экзамен 49-54 (п. 6.1) |
| | у9 | Способность диагностировать и устранять проблемы в работе серверов и сетевого оборудования Cisco, включая быстрое восстановление после сбоев. | Конспект лекций, Устный опрос (п. 5.1, вопросы 31-40) | Тест № 4 (п.6.2) |

² - для формулировки показателей использовать положения Таксономии Блума.

³ - Однотипные оценочные средства нумеруются, н-р: «Тест №2», «Контрольная работа №4».

⁴ - Примеры всех оценочных средств должны быть представлены в разделах 5,6.

⁵ - В скобках следует указать пункт разделов 5.6, в котором оно представлено.

4 Описание процедуры оценивания

Результаты обучения по профессиональному модулю, уровень сформированности компетенций оцениваются по четырёх бальной шкале оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Текущая аттестация по профессиональному модулю проводится с целью систематической проверки достижений обучающихся. Объектами оценивания являются: степень усвоения теоретических знаний, уровень овладения практическими умениями и навыками по всем видам учебной работы, качество выполнения самостоятельной работы, учебная дисциплина (активность на занятиях, своевременность выполнения различных видов заданий, посещаемость всех видов занятий по аттестуемой профессиональному модулю).

При проведении промежуточной аттестации оценивается достижение студентом запланированных по профессиональному модулю результатов обучения, обеспечивающих результаты освоения образовательной программы в целом.

Критерии оценивания устного ответа

(оценочные средства: *собеседование, устное сообщение, диспут, дискуссия, коллоквиум*)

5 баллов - ответ показывает прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры;

свободное владение монологической речью, логичность и последовательность ответа; умение приводить примеры современных проблем изучаемой области.

4 балла - ответ, обнаруживающий прочные знания основных процессов изучаемой предметной области, отличается глубиной и полнотой раскрытия темы; владение терминологическим аппаратом; умение объяснять сущность, явлений, процессов, событий, делать выводы и обобщения, давать аргументированные ответы, приводить примеры; свободное владение монологической речью, логичность и последовательность ответа. Однако допускается одна - две неточности в ответе.

3 балла – ответ, свидетельствующий в основном о знании процессов изучаемой предметной области, отличающийся недостаточной глубиной и полнотой раскрытия темы; знанием основных вопросов теории; слабо сформированными навыками анализа явлений, процессов, недостаточным умением давать аргументированные ответы и приводить примеры; недостаточно свободным владением монологической речью, логичностью и последовательностью ответа. Допускается несколько ошибок в содержании ответа; неумение привести пример развития ситуации, провести связь с другими аспектами изучаемой области.

2 балла – ответ, обнаруживающий незнание процессов изучаемой предметной области, отличающийся неглубоким раскрытием темы; незнанием основных вопросов теории, несформированными навыками анализа явлений, процессов; неумением давать аргументированные ответы, слабым владением монологической речью, отсутствием логичности и последовательности. Допускаются серьезные ошибки в содержании ответа; незнание современной проблематики изучаемой области.

Критерии оценивания письменной работы

(оценочные средства: реферат, эссе, конспект, контрольная работа, доклад (сообщение), в том числе выполненный в форме презентации, творческое задание, курсовая работа).

5 баллов - студент выразил своё мнение по сформулированной проблеме, аргументировал его, точно определив ее содержание и составляющие. Проблема раскрыта полностью, выводы обоснованы. Приведены данные отечественной и зарубежной литературы, статистические сведения, информация нормативно-правового характера. Студент владеет навыком самостоятельной работы по заданной теме; методами и приемами анализа теоретических и/или практических аспектов изучаемой области. Фактических ошибок, связанных с пониманием проблемы, нет; графически работа оформлена правильно.

4 балла - работа характеризуется смысловой цельностью, связностью и последовательностью изложения; допущено не более 1 ошибки при объяснении смысла или содержания проблемы. Проблема раскрыта. Не все выводы сделаны и/или обоснованы. Для аргументации приводятся данные отечественных и зарубежных авторов. Продемонстрированы исследовательские умения и навыки. Фактических ошибок, связанных с пониманием проблемы, нет. Допущены одна-две ошибки в оформлении работы.

3 балла – студент проводит достаточно самостоятельный анализ основных этапов и смысловых составляющих проблемы; понимает базовые основы и теоретическое обоснование выбранной темы. Проблема раскрыта не полностью. Выводы не сделаны и/или выводы не обоснованы. Проведен анализ проблемы без привлечения дополнительной литературы. Допущено не более 2 ошибок в смысле или содержании проблемы, оформлении работы.

2 балла - работа представляет собой пересказанный или полностью переписанный исходный текст без каких бы то ни было комментариев, анализа. Не раскрыта структура и теоретическая составляющая темы. Проблема не раскрыта. Выводы отсутствуют. Допущено три или более трех ошибок в смысловом содержании раскрываемой проблемы, в оформлении работы.

Критерии оценивания тестового задания

| Оценка | <i>Отлично</i> | <i>Хорошо</i> | <i>Удовлетворительно</i> | <i>Неудовлетворительно</i> |
|-------------------------------|----------------|------------------|--------------------------|----------------------------|
| Количество правильных ответов | 91 % и \geq | от 81% до 90,9 % | не менее 70% | менее 70% |

Критерии выставления оценки студенту на зачете/ экзамене

(оценочные средства: *устный опрос в форме ответов на вопросы билетов, устный опрос в форме собеседования, выполнение письменных разноуровневых задач и заданий и т.п.*)

| Оценка по промежуточной аттестации | Характеристика качества сформированности компетенций |
|--------------------------------------|--|
| «зачтено» / «отлично» | Студент демонстрирует сформированность дисциплинарных компетенций на продвинутом уровне: обнаруживает всестороннее, систематическое и глубокое знание учебного материала, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и другими видами применения знаний, причем не затрудняется с ответом при видоизменении заданий, правильно обосновывает принятое решение, владеет разносторонними навыками и приемами выполнения практических задач. |
| «зачтено» / «хорошо» | Студент демонстрирует сформированность дисциплинарных компетенций на базовом уровне: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации. |
| «зачтено» / «удовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций на пороговом уровне: имеет знания только основного материала, но не усвоил его деталей, в ходе контрольных мероприятий допускаются значительные ошибки, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ, при оперировании знаниями и умениями при их переносе на новые ситуации. |
| «не зачтено» / «неудовлетворительно» | Студент демонстрирует сформированность дисциплинарных компетенций на уровне ниже порогового: выявляется полное или практически полное отсутствие знаний значительной части программного материала, студент допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, умения и навыки не сформированы. |

5. Примеры оценочных средств для проведения текущей аттестации

5.1 Вопросы для собеседования (устного опроса):

1. Что такое Windows Server 2012 R2, и для чего он используется?
2. Какие основные роли и службы предоставляет Windows Server 2012 R2?
3. Каковы ключевые различия между Windows Server и клиентскими версиями Windows, такими как Windows 10?
4. Какие возможности предоставляются средствами управления сервером, такими как Server Manager и PowerShell?
5. Какие компоненты входят в группу ролей "Active Directory Domain Services" в Windows Server 2012 R2, и как они взаимодействуют?
6. Для чего используется служба DNS (Domain Name System) в Windows Server 2012 R2?
7. Что такое Hyper-V, и какие возможности виртуализации он предоставляет в Windows Server 2012 R2?
8. Какие меры безопасности и функции аутентификации предоставляются в Windows Server 2012 R2?
9. Как можно настроить резервное копирование и восстановление данных в Windows Server 2012 R2?
10. Какие требования к аппаратному обеспечению существуют для установки и использования Windows Server 2012 R2?
11. Что такое серверная операционная система, и какие задачи она выполняет на сервере?
12. Какие основные шаги следует предпринять при установке серверной операционной системы на физический сервер?
13. Какие виды установки операционной системы существуют, и когда каждый из них может быть использован?
14. Что такое роли сервера в контексте операционной системы Windows Server, и как они связаны с функциональностью сервера?
15. Какие базовые меры безопасности следует применять при настройке серверной операционной системы?
16. Какие инструменты управления и мониторинга доступны после установки операционной системы, и как они могут быть использованы для управления сервером?
17. Какие наиболее важные параметры и настройки нужно учесть при начальной настройке серверной операционной системы?
18. Какие роли и функции сервера можно добавить или убрать после установки операционной системы, и как это делается?
19. Какие рекомендации можно дать по созданию резервных копий и восстановлению данных при настройке серверной операционной системы?
20. Какие методы и инструменты мониторинга производительности можно использовать для отслеживания работы сервера и выявления возможных проблем?
21. Что такое маршрутизатор Cisco, и какие функции он выполняет в сети?
22. Какие основные протоколы маршрутизации поддерживаются на устройствах Cisco, и как они работают?
23. Какие коммутаторы Cisco, и какие задачи они решают в локальных сетях?
24. Как настроить виртуальное LAN (VLAN) на коммутаторе Cisco?
25. Какие меры безопасности можно применить на маршрутизаторах и коммутаторах Cisco для защиты сети?
26. Какие основные шаги необходимо выполнить при настройке маршрутизатора Cisco для доступа к Интернету?
27. Как управлять списками доступа (ACL) на маршрутизаторе Cisco для контроля трафика?
28. Какие инструменты и протоколы используются для мониторинга и управления сетевыми устройствами Cisco?

29. Как настроить каналы агрегации (EtherChannel) на коммутаторах Cisco для повышения пропускной способности?
30. Как выполнить резервное копирование конфигурации устройства Cisco, и как восстановить ее в случае сбоя?
31. Что такое лог-файлы (журналы событий) в операционной системе Cisco IOS, и как они могут помочь в диагностике сетевых проблем?
32. Какие основные принципы работы протокола SNMP (Simple Network Management Protocol) и как он используется для мониторинга и диагностики сетевых устройств Cisco?
33. Какие команды и инструменты можно использовать для проверки соединения между двумя сетевыми устройствами Cisco?
34. Что такое протоколы ICMP и какие команды ICMP используются для проверки доступности сетевых устройств?
35. Какие методы обеспечивают высокую доступность серверов и сетевого оборудования Cisco, и какие шаги следует предпринять при возникновении сбоев для быстрого восстановления?
36. Какие меры безопасности следует соблюдать при удаленной диагностике и управлении сетевыми устройствами Cisco?
37. Какие методы диагностики сетевых проблем можно применить с использованием команды "ping" в операционной системе Cisco IOS?
38. Что такое протоколы HSRP (Hot Standby Router Protocol) и VRRP (Virtual Router Redundancy Protocol), и как они обеспечивают высокую доступность в сетях Cisco?
39. Какие типичные сценарии сбоев могут возникнуть при работе сетевых устройств Cisco, и какие шаги нужно предпринять для их устранения?
40. Какие преимущества и недостатки связаны с применением системы мониторинга сетевых устройств Cisco, такой как Cisco Prime Infrastructure, для диагностики и управления сетью?

5.2 Примеры тестовых заданий:

Тест № 1

Вариант 1

1. Какой из перечисленных методов установки Windows Server 2012 R2 подразумевает использование образа операционной системы и DVD-диска?
 - a. Установка сетевого образа;
 - b. Установка с использованием WDS;
 - c. Установка с физического носителя;
 - d. Установка с использованием PowerShell.
2. Какие базовые системные требования необходимы для успешной установки Windows Server 2012 R2?
 - a. Процессор Intel Pentium III;
 - b. Минимум 1 ГБ оперативной памяти;
 - c. Минимум 32 ГБ свободного места на диске;
 - d. Видеокарта с поддержкой DirectX 9.
3. Какие компоненты можно установить во время настройки ролей и функций после установки Windows Server 2012 R2?
 - a. Исполнительные файлы;
 - b. Прокси-сервер;
 - c. Службы удаленного рабочего стола;
 - d. Игровые приложения.

Вариант 2

1. Какой из методов установки Windows Server 2012 R2 позволяет создать виртуальную машину на хост-системе и установить на нее ОС?
 - a. Установка сетевого образа;
 - b. Установка с использованием WDS;
 - c. Установка на виртуальную машину;
 - d. Установка с использованием PowerShell.
2. Что такое роли сервера в контексте операционной системы Windows Server 2012 R2?
 - a. Готовые приложения для сервера;
 - b. Разрешения на доступ к данным;
 - c. Функциональные компоненты, которые определяют функции сервера;
 - d. Пользовательские настройки сервера.
3. Какой метод настройки серверной роли является наиболее безопасным?
 - a. Автоматическая настройка;
 - b. Полуавтоматическая настройка;
 - c. Ручная настройка;
 - d. Отключение роли после установки.

Вариант 3

1. Какой тип установки Windows Server 2012 R2 обычно используется для физических серверов с несколькими дисками?
 - a. С установкой сетевого образа;
 - b. С установкой с использованием WDS;
 - c. С пользовательской установкой;
 - d. С установкой на несколько дисков.
2. Что такое DHCP, и зачем он используется при установке серверной операционной системы?
 - a. Протокол для установки пароля администратора;
 - b. Протокол для автоматической настройки сетевых параметров;
 - c. Протокол для установки антивирусного ПО;
 - d. Протокол для удаленного управления сервером.
3. Как можно установить дополнительные компоненты и роли на сервере Windows Server 2012 R2 после базовой установки?
 - a. С помощью BIOS-настроек;
 - b. С помощью инсталляционного диска;
 - c. Через командную строку PowerShell;
 - d. С помощью утилиты CHKDSK.

Ответы на тест № 1:

Вариант 1:

- Вопрос 1: с
Вопрос 2: с
Вопрос 3: с

Вариант 2:

- Вопрос 1: с
- Вопрос 2: с
- Вопрос 3: с

Вариант 3:

- Вопрос 1: с
- Вопрос 2: b
- Вопрос 3: с

Время выполнения – 30 минут.

Тест № 2

Вариант 1

1. Какой командой можно создать новую директорию в Linux?
 - a. ``cd``
 - b. ``mkdir``
 - c. ``touch``
 - d. ``rm``
2. Какая команда используется для просмотра списка процессов, работающих в системе?
 - a. ``ps``
 - b. ``ls``
 - c. ``top``
 - d. ``kill``
3. Какие команды используются для установки нового программного обеспечения в Linux через командную строку?
 - a. ``apt-get`` и ``yum``
 - b. ``mkdir`` и ``touch``
 - c. ``ls`` и ``cd``
 - d. ``grep`` и ``sed``
4. Какие типы прав доступа существуют в Linux?
 - a. Только "чтение" и "запись"
 - b. Только "чтение", "запись" и "исполнение"
 - c. "Чтение", "запись" и "исполнение" для владельца, группы и остальных пользователей
 - d. Только "исполнение"
5. Какие команды используются для настройки сетевых параметров, таких как IP-адрес, в Linux?
 - a. ``network-config`` и ``ip-setup``
 - b. ``ifconfig`` и ``netstat``
 - c. ``ping`` и ``traceroute``
 - d. ``ssh`` и ``telnet``
6. Какие команды позволяют вам изменить права доступа к файлу или директории в Linux?
 - a. ``chown`` и ``chmod``
 - b. ``mv`` и ``cp``
 - c. ``grep`` и ``sed``
 - d. ``pwd`` и ``ls``

Вариант 2

1. Какой командой можно создать новую директорию в Linux?
 - a. ``cd``
 - b. ``mkdir``
 - c. ``touch``
 - d. ``rm``
2. Какая команда используется для просмотра списка процессов, работающих в системе?
 - a. ``ps``
 - b. ``ls``
 - c. ``top``
 - d. ``kill``
3. Какие команды используются для установки нового программного обеспечения в Linux через командную строку?
 - a. ``apt-get`` и ``yum``
 - b. ``mkdir`` и ``touch``
 - c. ``ls`` и ``cd``
 - d. ``grep`` и ``sed``
4. Какие типы прав доступа существуют в Linux?
 - a. Только "чтение" и "запись"
 - b. Только "чтение", "запись" и "исполнение"
 - c. "Чтение", "запись" и "исполнение" для владельца, группы и остальных пользователей
 - d. Только "исполнение"
5. Какие команды используются для настройки сетевых параметров, таких как IP-адрес, в Linux?
 - a. ``network-config`` и ``ip-setup``
 - b. ``ifconfig`` и ``netstat``
 - c. ``ping`` и ``traceroute``
 - d. ``ssh`` и ``telnet``
6. Какие команды позволяют вам изменить права доступа к файлу или директории в Linux?
 - a. ``chown`` и ``chmod``
 - b. ``mv`` и ``cp``
 - c. ``grep`` и ``sed``
 - d. ``pwd`` и ``ls``

Вариант 3

1. Какой командой можно создать новую директорию в Linux?
 - a. ``cd``
 - b. ``mkdir``
 - c. ``touch``
 - d. ``rm``
2. Какая команда используется для просмотра списка процессов, работающих в системе?
 - a. ``ps``
 - b. ``ls``
 - c. ``top``
 - d. ``kill``
3. Какие команды используются для установки нового программного обеспечения в Linux через командную строку?
 - a. ``apt-get`` и ``yum``
 - b. ``mkdir`` и ``touch``
 - c. ``ls`` и ``cd``
 - d. ``grep`` и ``sed``
4. Какие типы прав доступа существуют в Linux?

- a. Только "чтение" и "запись"
 - b. Только "чтение", "запись" и "исполнение"
 - c. "Чтение", "запись" и "исполнение" для владельца, группы и остальных пользователей
 - d. Только "исполнение"
5. Какие команды используются для настройки сетевых параметров, таких как IP-адрес, в Linux?
- a. ``network-config`` и ``ip-setup``
 - b. ``ifconfig`` и ``netstat``
 - c. ``ping`` и ``traceroute``
 - d. ``ssh`` и ``telnet``
6. Какие команды позволяют вам изменить права доступа к файлу или директории в Linux?
- a. ``chown`` и ``chmod``
 - b. ``mv`` и ``cp``
 - c. ``grep`` и ``sed``
 - d. ``pwd`` и ``ls``

Ответы на тест № 1:

- Вариант 1: b
- Вариант 1: a
- Вариант 1: a
- Вариант 1: c
- Вариант 1: b
- Вариант 1: a

Тест № 3

Вариант 1

1. Какие основные сетевые параметры вы можете настроить на клиентском компьютере для подключения к сети?
- a. Имя пользователя и пароль
 - b. IP-адрес и маску подсети
 - c. Разрешение экрана и цветовую гамму
 - d. Маршрутизатор и DNS-сервер
2. Какие инструменты вы используете для диагностики сетевых проблем на клиентском компьютере?
- a. Программа для просмотра фотографий
 - b. Клиент электронной почты
 - c. Командная строка и сетевые команды
 - d. Веб-браузер
3. Что может быть причиной отсутствия подключения к интернету на клиентском компьютере, даже если сетевые параметры правильно настроены?
- a. Проблемы с процессором
 - b. Неправильная цветовая гамма
 - c. Отключен антивирусный программный продукт
 - d. Неисправности на маршрутизаторе или провайдере интернет-соединения
4. Какая команда используется для проверки доступности удаленного сервера по его IP-адресу?
- a. ``ping``
 - b. ``ls``
 - c. ``cd``
 - d. ``mv``

5. Как можно устранить проблему, если клиентский компьютер не может найти нужную веб-страницу?
 - a. Перезагрузить компьютер
 - b. Проверить правильность URL-адреса
 - c. Заменить жесткий диск
 - d. Отключить сетевой адаптер
6. Какие инструменты и методы вы используете для мониторинга и анализа сетевого трафика на клиентском компьютере?
 - a. Факс и сканер
 - b. Веб-камера и микрофон
 - c. Сетевые анализаторы и программы мониторинга
 - d. Системный диспетчер Windows
7. Какие шаги вы предпримете, чтобы защитить клиентский компьютер от вредоносных программ и атак из сети?
 - a. Установить более мощный процессор
 - b. Постоянно выключать компьютер
 - c. Установить антивирусное программное обеспечение и обновлять его
 - d. Изменить цвет рабочего стола
8. Какие проблемы могут возникнуть при подключении клиентского компьютера к беспроводной сети?
 - a. Проблемы с монитором
 - b. Отсутствие звука
 - c. Интерференция и слабый сигнал Wi-Fi
 - d. Низкая яркость экрана
9. Какие основные шаги вы предпримете, чтобы настроить электронную почту на клиентском компьютере?
 - a. Подключить принтер
 - b. Вставить флеш-накопитель
 - c. Ввести параметры почтового сервера и учетные данные
 - d. Проверить батарею
10. Какие действия вы предпримете, если клиентская инфраструктура подверглась атаке хакера?
 - a. Попытаться атаковать хакера в ответ
 - b. Срочно выключить компьютеры
 - c. Изолировать компьютеры от сети, изменить пароли и провести анализ инцидента
 - d. Запустить сетевой брандмауэр

Вариант 2

1. Какие основные сетевые параметры вы можете настроить на клиентском компьютере для подключения к сети?
 - a. Размер оперативной памяти
 - b. MAC-адрес сетевой карты
 - c. Имя компьютера
 - d. IP-адрес и маску подсети
2. Какие инструменты вы используете для диагностики сетевых проблем на клиентском компьютере?
 - a. Телефон и факс
 - b. Веб-камера и микрофон
 - c. Командная строка и сетевые команды
 - d. Программа для просмотра фотографий
3. Что может быть причиной отсутствия подключения к интернету на клиентском компьютере, даже если сетевые параметры правильно настроены?

- a. Проблемы с жестким диском
 - b. Неправильная цветовая гамма
 - c. Отключен антивирусный программный продукт
 - d. Неисправности на маршрутизаторе или провайдере интернет-соединения
4. Какая команда используется для проверки доступности удаленного сервера по его IP-адресу?
- a. `ping`
 - b. `ls`
 - c. `cd`
 - d. `mv`
5. Как можно устранить проблему, если клиентский компьютер не может найти нужную веб-страницу?
- a. Заменить монитор
 - b. Проверить правильность URL-адреса
 - c. Заменить оперативную память
 - d. Отключить сетевой адаптер
6. Какие инструменты и методы вы используете для мониторинга и анализа сетевого трафика на клиентском компьютере?
- a. Веб-браузер и почтовый клиент
 - b. Сетевые анализаторы и программы мониторинга
 - c. Системный диспетчер Windows
 - d. Программа для редактирования изображений
7. Какие шаги вы предпримете, чтобы защитить клиентский компьютер от вредоносных программ и атак из сети?
- a. Установить больше оперативной памяти
 - b. Изменить стандартный фон рабочего стола
 - c. Установить антивирусное программное обеспечение и обновлять его
 - d. Подключить дополнительные мониторы
8. Какие проблемы могут возникнуть при подключении клиентского компьютера к беспроводной сети?
- a. Проблемы с клавиатурой
 - b. Отсутствие аудиосистемы
 - c. Интерференция и слабый сигнал Wi-Fi
 - d. Низкое разрешение экрана
9. Какие основные шаги вы предпримете, чтобы настроить электронную почту на клиентском компьютере?
- a. Подключить принтер
 - b. Вставить флеш-накопитель
 - c. Ввести параметры почтового сервера и учетные данные
 - d. Запустить сетевой брандмауэр
10. Какие действия вы предпримете, если клиентская инфраструктура подверглась атаке хакера?
- a. Оставить компьютер включенным и наблюдать за действиями хакера
 - b. Выключить компьютер и связаться с экспертом по компьютерной безопасности
 - c. Изменить пароли и провести анализ инцидента
 - d. Удалить все программное обеспечение

Ответы на тест № 1:

Вариант 1:

- 1. Вопрос 1: b
- 2. Вопрос 2: c
- 3. Вопрос 3: d

4. Вопрос 4: a
5. Вопрос 5: b
6. Вопрос 6: c
7. Вопрос 7: c
8. Вопрос 8: c
9. Вопрос 9: c
10. Вопрос 10: c

Вариант 2:

1. Вопрос 1: d
2. Вопрос 2: c
3. Вопрос 3: d
4. Вопрос 4: a
5. Вопрос 5: b
6. Вопрос 6: b
7. Вопрос 7: c
8. Вопрос 8: c
9. Вопрос 9: c
10. Вопрос 10: b

5.3 Практические задания:

Практическое задание № 1: Настройка и управление службами сетевых протоколов в Windows Server 2012 R2

Цель задания: Освоить процесс настройки и управления службами сетевых протоколов, такими как DNS и DHCP, в операционной системе Windows Server 2012 R2.

Инструкции:

Часть 1: Настройка DNS

1. Создайте виртуальную машину (VM) в вашей виртуализационной среде (например, VirtualBox, VMware, Hyper-V) с установленной Windows Server 2012 R2.
2. Установите роль DNS-сервера на вашем сервере. Убедитесь, что вы правильно настроили зону "Прямого поиска" (Forward Lookup Zone) для вашей внутренней сети.
3. Создайте несколько записей DNS, включая записи A и записи CNAME.
4. Убедитесь, что DNS-сервер правильно разрешает имена для узлов в вашей сети.

Часть 2: Настройка DHCP

5. Настройте роль DHCP-сервера на вашем Windows Server 2012 R2. Создайте DHCP-пул и укажите параметры аренды IP-адресов.
6. Подключите виртуальную машину (например, клиентскую машину) к сети и настройте ее для автоматического получения IP-адреса через DHCP.
7. Проверьте, что клиентская машина успешно получила IP-адрес, а также информацию о шлюзе и DNS-сервере.

Часть 3: Дополнительные задачи

8. Создайте резервацию DHCP для определенного устройства, чтобы оно всегда получало тот же IP-адрес.
9. Настройте фильтрацию MAC-адресов в DHCP-сервере, чтобы предотвратить выдачу IP-адресов определенным устройствам.
10. Убедитесь, что сервер успешно выполняет обновление DNS-записей для клиентских машин, получивших IP-адрес через DHCP.
11. Создайте запись PTR (обратной записи) для одного из IP-адресов, используемых в вашей сети.
12. Ответьте на вопросы, связанные с процессом настройки и управления DNS и DHCP на вашем сервере.

Замечание: Это практическое задание позволит студентам овладеть навыками настройки и управления службами сетевых протоколов DNS и DHCP в Windows Server 2012 R2.

Время выполнения – 90 минут.

Практическое задание № 2: Настройка и управление службами сетевых протоколов в Windows Server 2012 R2

Цель задания: Овладеть навыками диагностики и устранения проблем, возникающих в Linux, с использованием стандартных инструментов командной строки.

Инструкции:

1. *Проблема с сетью:*
 - Создайте виртуальную машину с Linux (возможно, используя VirtualBox или другую виртуализационную платформу).
 - Настройте виртуальную машину так, чтобы у нее не было доступа к сети (например, отключите сетевой адаптер).
 - Запустите виртуальную машину и попробуйте установить, в чем заключается проблема с сетью.
 - Используйте команды `ifconfig`, `ping`, `netstat`, и `route`, чтобы диагностировать и устранить проблему с сетью.
2. *Проблема с диском:*
 - Создайте виртуальную машину с Linux.
 - Создайте виртуальный жесткий диск для этой машины и назначьте ему недостаточное количество места (например, 1 ГБ).
 - Запустите виртуальную машину и попробуйте выполнить какие-либо операции, требующие дополнительного места на диске (например, установку пакетов).
 - Используйте команды `df`, `du`, и `rm`, чтобы диагностировать и устранить проблему с диском.
3. *Проблема с процессами:*
 - Создайте виртуальную машину с Linux.
 - Запустите несколько процессов, например, приложений, искусственно увеличьте их потребление ресурсов (например, с помощью команды `stress`).
 - Используйте команды `top`, `ps`, и `kill`, чтобы диагностировать и устранить проблему с процессами, например, завершите зависший процесс.
4. *Проблема с правами доступа:*
 - Создайте директорию и файл в Linux и настройте неправильные права доступа к ним.
 - Попробуйте выполнить операции чтения, записи и выполнения с этими файлами и директориями.
 - Используйте команды `ls`, `chmod`, и `chown`, чтобы диагностировать и устранить проблему с правами доступа.
5. *Проблема с DNS:*
 - Создайте виртуальную машину с Linux и настройте ее DNS-серверы на неверные значения.
 - Попробуйте выполнить DNS-запросы (например, `nslookup` или `ping`) для веб-сайтов и серверов.
 - Используйте команды `cat`, `vi`, или `nano`, чтобы отредактировать файл с настройками DNS (обычно `/etc/resolv.conf`) и устранить проблему.
6. *Проблема с загрузкой:*
 - Создайте виртуальную машину с Linux и модифицируйте файл загрузки (например, `/etc/fstab`) так, чтобы система не могла корректно загрузиться (например, неверный путь к корневой файловой системе).

- Попробуйте перезагрузить систему и убедитесь, что она не загружается.
- Используйте команду `grub` или другие средства загрузки для восстановления загрузки.

Замечания:

- В каждом случае, вашей целью является диагностика и устранение проблемы, а также документирование шагов, предпринятых для решения проблемы.
- По завершении каждой задачи, предоставьте отчет, описывающий проблему, принятые меры и результаты.
- Это практическое задание поможет вам освоить навыки диагностики и устранения проблем, которые могут возникнуть на серверах и рабочих станциях Linux.

Время выполнения – 90 минут.

Практическое задание № 3: Анализ и оптимизация сетевой инфраструктуры организации

Цель задания: Провести анализ сетевой инфраструктуры организации, выявить её слабые места и предложить оптимизационные меры для улучшения производительности и безопасности.

Необходимые ресурсы:

1. Доступ к сетевой инфраструктуре организации (локальной сети, серверам, маршрутизаторам).
2. Доступ к схемам сетевой инфраструктуры (если доступны).
3. Компьютер для анализа и документирования результатов.

Шаги выполнения:

1. *Сбор информации:*
 - Соберите информацию о текущей сетевой инфраструктуре организации, включая сетевую топологию, используемое оборудование (маршрутизаторы, коммутаторы), сетевые сервисы (DNS, DHCP), структуру сетей (внутренние и внешние), текущие пропускные способности и т.д.
2. *Анализ производительности:*
 - Проведите анализ производительности сети. Измерьте скорость передачи данных между узлами сети и выявите узкие места.
 - Оцените нагрузку на сеть и пропускную способность каналов связи.
3. *Анализ безопасности:*
 - Проверьте текущие меры безопасности, используемые в сети (файрволы, антивирусные решения, VPN и т.д.).
 - Оцените сетевую уязвимость и выявите потенциальные точки доступа для несанкционированных пользователей.
4. *Оптимизация и рекомендации:*
 - На основе собранной информации и результатов анализа, предложите конкретные меры по оптимизации сетевой инфраструктуры и повышению безопасности.
 - Ваши рекомендации могут включать в себя модернизацию оборудования, настройку балансировки нагрузки, улучшение сетевых сервисов и реализацию дополнительных мер безопасности.
5. *Составление отчета:*
 - Составьте подробный отчет, включающий информацию о текущем состоянии сети, выявленных проблемах, рекомендациях по оптимизации и безопасности.
 - Презентуйте свои рекомендации организации или предоставьте их руководству.
6. *Обсуждение и демонстрация:*

- Проведите обсуждение результатов анализа и рекомендаций с коллегами или руководством организации.
- Предоставьте демонстрацию возможных изменений и улучшений в сетевой инфраструктуре.

Замечание: Это практическое задание позволит студентам применить знания по анализу и оптимизации сетевой инфраструктуры в реальной организации. Это также способствует развитию навыков планирования и рекомендации улучшений для повышения производительности и безопасности сети.

Время выполнения – 90 минут.

5.4 Примеры заданий для контрольной работы:

Контрольная работа № 1: Процессы резервного копирования и восстановления данных на сервере

Вариант 1

1. Что такое резервное копирование данных на сервере и какая его цель?
2. Какие виды резервного копирования данных существуют, и как они отличаются друг от друга?
3. Что такое политика резервного копирования, и какие факторы могут влиять на ее выбор?
4. Какие компоненты серверной системы обычно включают в процесс резервного копирования?
5. Какой метод резервного копирования наиболее подходит для восстановления данных в случае их повреждения: полное, дифференциальное или инкрементное?
6. Какие технологии и средства Windows Server используются для управления резервным копированием?
7. Какие наиболее важные шаги следует предпринять при создании плана восстановления данных (DRP) для сервера?
8. Какие типы носителей можно использовать для хранения резервных копий, и какой из них наиболее надежен и удобен?
9. Что такое тестирование восстановления, и почему оно важно для процесса резервного копирования?
10. Каковы наилучшие практики по мониторингу и обслуживанию системы резервного копирования на сервере?

Вариант 2

1. Что представляет собой процесс восстановления данных на сервере и почему он так важен для бизнеса?
2. Какие данные на сервере обычно подлежат резервному копированию, и как определить их важность?
3. Какова роль графического интерфейса и командной строки в процессе настройки резервного копирования на сервере?
4. Какие виды резервного копирования данных существуют, и в чем их преимущества и недостатки?
5. Какие основные компоненты и службы Windows Server используются для выполнения операций резервного копирования?
6. В чем заключается разница между локальным и удаленным хранением резервных копий, и какие факторы влияют на выбор места хранения?
7. Какой метод восстановления данных наиболее эффективен для восстановления сервера после сбоя: полное восстановление, восстановление по частям или альтернативный метод?

8. Какие наиболее распространенные угрозы для данных на сервере могут потребовать использования резервных копий?
9. Что такое RTO (Recovery Time Objective) и RPO (Recovery Point Objective), и как они связаны с процессами резервного копирования и восстановления?
10. Какие процедуры и меры обслуживания системы резервного копирования необходимо выполнять регулярно, чтобы обеспечить ее надежную работу?

Эти вопросы охватывают основные аспекты резервного копирования и восстановления данных на сервере и помогут оценить способность студентов понимать этот процесс.

Контрольная работа № 2: Методы мониторинга и диагностики состояния сервера

Вариант 1

1. Перечислите основные методы мониторинга производительности сервера.
2. Что такое SNMP, и как он используется для мониторинга серверов?
3. Какие виды событий и журналов событий Windows можно использовать для диагностики проблем на сервере?
4. Какие инструменты и утилиты входят в состав Windows для мониторинга и диагностики сервера?
5. Что такое анализатор производительности (Performance Monitor), и как он может быть использован для мониторинга сервера?
6. Какие метрики и показатели производительности следует отслеживать при мониторинге сервера баз данных?
7. Что такое аудит событий, и для чего он используется в контексте мониторинга и безопасности сервера?
8. Какие протоколы и инструменты можно использовать для мониторинга сетевого трафика на сервере?
9. Что такое централизованный мониторинг серверов, и какие преимущества он может предоставить в больших сетях?
10. Какие методы мониторинга доступны для серверов виртуализации, таких как Hyper-V?

Вариант 2

1. Какие виды мониторинга существуют для отслеживания состояния серверов?
2. Что такое агентный и агент-лесс мониторинг, и в чем их основные различия?
3. Как можно настроить мониторинг метрик производительности с использованием системы Zabbix?
4. Какие роли выполняют системы регистрации (logging) в мониторинге и диагностике сервера?
5. Какие показатели производительности следует отслеживать при работе с серверами баз данных (например, SQL Server)?
6. Какие инструменты и технологии могут использоваться для мониторинга безопасности сервера?
7. Как можно настроить мониторинг событий в системе Windows Server с использованием службы сбора событий (Event Collector)?
8. Какие методы мониторинга можно использовать для обнаружения атак на сетевой уровень сервера?
9. Какие преимущества предоставляет облачный мониторинг серверов, и какие инструменты позволяют его реализовать?
10. Какие меры предпринимаются для обеспечения безопасности и конфиденциальности данных при мониторинге серверов?

Эти вопросы охватывают основные аспекты мониторинга и диагностики состояния сервера и могут быть использованы для проверки знаний студентов на эту тему.

Контрольная работа № 3: Методы мониторинга и диагностики состояния сервера

Вариант 1

1. Что такое групповая политика (Group Policy) в операционных системах Windows, и какие задачи она позволяет выполнять?
2. Какие основные компоненты групповой политики существуют, и как они взаимодействуют между собой?
3. Как можно создать новую групповую политику в Active Directory, и какие настройки она может включать?
4. Какие типичные задачи можно решать с помощью групповой политики для настольных приложений?
5. Что такое "Объекты политики безопасности" (Security Policy Objects) в контексте групповой политики, и как они используются?
6. Как можно назначить групповую политику для определенных пользователей или компьютеров в сети?
7. Как происходит применение групповой политики на клиентских системах, и в какой последовательности выполняются настройки?
8. Какие инструменты и утилиты можно использовать для управления групповой политикой на сервере Windows?
9. Какие меры безопасности и резервного копирования рекомендуется применять при работе с групповой политикой?
10. Какие типичные проблемы могут возникать при настройке и управлении групповой политикой, и как их можно решить?

Вариант 2

1. Что такое групповая политика (Group Policy) в операционных системах Windows, и какие задачи она позволяет выполнять?
2. Какие основные компоненты групповой политики существуют, и как они взаимодействуют между собой?
3. Как можно создать новую групповую политику в Active Directory, и какие настройки она может включать?
4. Какие типичные задачи можно решать с помощью групповой политики для клиентских систем и настольных приложений?
5. Что такое "Объекты политики безопасности" (Security Policy Objects) в контексте групповой политики, и как они используются?
6. Как можно назначить групповую политику для определенных пользователей или компьютеров в сети?
7. Как происходит применение групповой политики на клиентских системах, и в какой последовательности выполняются настройки?
8. Какие инструменты и утилиты можно использовать для управления групповой политикой на сервере Windows?
9. Какие меры безопасности и резервного копирования рекомендуется применять при работе с групповой политикой?
10. Какие типичные проблемы могут возникать при настройке и управлении групповой политикой, и как их можно решить?

Эти вопросы охватывают основные аспекты мониторинга и диагностики состояния сервера и могут быть использованы для проверки знаний студентов на эту тему.

Контрольная работа № 4: Методы мониторинга и диагностики состояния сервера

Вариант 1

1. Что такое высокая доступность в контексте серверов и сетей?

2. Какой метод обеспечения высокой доступности используется для создания группы серверов, которые работают параллельно и могут заменять друг друга в случае сбоя?
3. Какая технология обеспечивает отказоустойчивость коммутаторов Cisco путем создания виртуального устройства?
4. Какое преимущество предоставляет использование кластеров серверов Linux для обеспечения высокой доступности?
5. Какой протокол обычно используется для обеспечения согласованности данных между узлами кластера серверов?
6. Что представляет собой резервное копирование данных с целью их сохранения в случае сбоя или потери?
7. Какие технологии используются для обеспечения отказоустойчивости в виртуальных средах на базе Linux?
8. Какое преимущество предоставляет использование балансировки нагрузки в кластере серверов?
9. Какая команда в Linux используется для резервирования IP-адреса для определенного сетевого устройства?
10. Какие методы обеспечения высокой доступности следует использовать в сочетании для максимальной надежности системы?

Вариант 2

1. Что такое высокая доступность в контексте серверов и сетей?
2. Какой метод обеспечения высокой доступности используется для создания группы серверов, которые работают параллельно и могут заменять друг друга в случае сбоя?
3. Какая технология обеспечивает отказоустойчивость коммутаторов Cisco путем создания виртуального устройства?
4. Какое преимущество предоставляет использование кластеров серверов Linux для обеспечения высокой доступности?
5. Какой протокол обычно используется для обеспечения согласованности данных между узлами кластера серверов?
6. Что представляет собой резервное копирование данных с целью их сохранения в случае сбоя или потери?
7. Какие технологии используются для обеспечения отказоустойчивости в виртуальных средах на базе Linux?
8. Какое преимущество предоставляет использование балансировки нагрузки в кластере серверов?
9. Какая команда в Linux используется для резервирования IP-адреса для определенного сетевого устройства?
10. Какие методы обеспечения высокой доступности следует использовать в сочетании для максимальной надежности системы?

5.5 Темы докладов (рефератов и сообщений):

1. Введение в командную строку Linux: основные понятия и преимущества.
2. Основные команды работы с файлами и директориями в Linux.
3. Практические навыки навигации и манипуляции в командной строке Linux.
4. Управление пользователями и правами доступа в Linux через командную строку.
5. Автоматизация задач с помощью сценариев командной строки в Linux.
6. Использование команд для мониторинга и управления процессами в Linux.
7. Сетевые команды и настройка сетевых параметров в командной строке Linux.
8. Работа с архивами и сжатием файлов через командную строку Linux.
9. Основы системного администрирования Linux через командную строку.
10. Безопасность и защита данных в Linux: команды и концепции.
11. Протокол IPv6: Переход к следующему поколению IP-адресации.

12. SD-WAN (Software-Defined Wide Area Network): Преимущества и реализация.
13. 5G и будущее мобильной связи.
14. Стандарты Wi-Fi 6 (802.11ax) и Wi-Fi 6E.
15. IoT (Internet of Things): Сети для подключенных устройств.
16. Принципы и преимущества виртуализации сетей.
17. Применение технологии Docker в сетевых приложениях.
18. Протоколы сетевой безопасности: IPsec и SSL/TLS.
19. Топологии сетей для предприятий: от классических до современных.
20. Искусственный интеллект (ИИ) в сетевой безопасности.
21. Использование RESTful API для взаимодействия с сетевой инфраструктурой в настольных приложениях.
22. Применение библиотек и фреймворков для разработки клиент-серверных настольных приложений.
23. Интеграция WebSocket для обеспечения реального времени в настольных приложениях.
24. Разработка настольных приложений с поддержкой многопоточности для оптимального взаимодействия с сетевой инфраструктурой.
25. Безопасность в настольных приложениях: методы обеспечения защиты данных при взаимодействии с сетью.
26. Использование прокси-серверов для оптимизации работы настольных приложений в сети.
27. Интеграция сетевых протоколов, таких как HTTP, FTP, и SMTP, в настольные приложения.
28. Принципы асинхронного взаимодействия в сетевых настольных приложениях.
29. Работа с форматами данных, такими как JSON и XML, в настольных приложениях при обмене информацией по сети.
30. Оптимизация производительности сетевых настольных приложений: советы и методы.
31. Основы безопасности настольных приложений: как защитить данные пользователя.
32. Использование паролей и аутентификации для обеспечения безопасности в настольных приложениях.
33. Роль обновлений и патчей в защите настольных приложений.
34. Антивирусное программное обеспечение и антималваре для настольных приложений.
35. Защита данных в памяти и при передаче через сеть в настольных приложениях.
36. Методы обнаружения и предотвращения атак на настольные приложения.
37. Работа с разрешениями и правами доступа в настольных приложениях.
38. Сетевая безопасность и настольные приложения: основные меры и принципы.
39. Шифрование данных в настольных приложениях: зачем и как.
40. Советы по обеспечению безопасности при разработке и развертывании настольных приложений.
41. Основы архитектуры сетевых серверов Cisco.
42. Установка и начальная настройка сервера Cisco.
43. Конфигурация маршрутизации на серверах Cisco.
44. Настройка безопасности сетевых серверов Cisco.
45. Управление пользовательскими учетными записями на серверах Cisco.
46. Настройка сервисов и приложений на серверах Cisco.
47. Резервное копирование и восстановление данных на серверах Cisco.
48. Мониторинг и диагностика состояния серверов Cisco.
49. Обновление и планирование обслуживания серверов Cisco.
50. Интеграция сетевых серверов Cisco в общую инфраструктуру.

6. Примеры оценочных средств для проведения промежуточной аттестации

6.1 Варианты экзаменационных билетов:

1. Какие роли сервера могут быть установлены в Windows Server 2012 R2, и какова их роль в обеспечении функциональности сервера?
2. Как настроить службу Active Directory Domain Services в Windows Server 2012 R2 и какие основные задачи она выполняет?
3. Объясните, как настроить и использовать службу DHCP (Dynamic Host Configuration Protocol) в Windows Server 2012 R2 для управления IP-адресами в сети.
4. Что такое Hyper-V в Windows Server 2012 R2, и какие преимущества он предоставляет для виртуализации серверов?
5. Какие инструменты управления и мониторинга доступны в Windows Server 2012 R2, и как их использовать для обеспечения стабильной работы сервера?
6. Какие меры безопасности и методы аутентификации можно настроить в Windows Server 2012 R2, чтобы защитить сервер и данные от угроз?
7. Какие шаги следует предпринять при установке серверной операционной системы на физический сервер?
8. Чем отличается установка операционной системы с нуля от обновления существующей системы? Какие факторы могут повлиять на выбор метода установки?
9. Какие роли сервера можно установить в операционной системе Windows Server, и как это делается?
10. Какие параметры безопасности следует учесть при начальной настройке серверной операционной системы?
11. Какие инструменты и ресурсы доступны для резервного копирования и восстановления данных на сервере?
12. Какие методы мониторинга производительности могут быть использованы для отслеживания работы сервера после установки и настройки операционной системы?
13. Что такое командная строка Linux и какую роль она играет в операционной системе?
14. Как вы перейдете из одной директории в другую с использованием командной строки Linux?
15. Какие команды используются для создания новой пустой директории и файла в Linux?
16. Что такое абсолютный и относительный путь в Linux, и как они отличаются друг от друга?
17. Какие команды позволяют вам просматривать содержимое файла в командной строке Linux?
18. Как вы удаляете файл или директорию с помощью командной строки Linux?
19. Какие команды вы используете для просмотра содержимого текущей директории в командной строке Linux?
20. Как можно создать новый пользовательский аккаунт в Linux, и какие права доступа можно назначить этому пользователю?
21. Как изменить пароль для существующего пользователя в Linux?
22. Какие команды позволяют вам настраивать сетевые параметры, такие как IP-адрес, в Linux?
23. Что такое DHCP и как его настроить в Linux для автоматической выдачи IP-адресов клиентам?
24. Какие команды используются для управления процессами в Linux, включая запуск, приостановку и завершение процессов?
25. Какие основные преимущества протокола IPv6 по сравнению с IPv4, и почему переход к IPv6 становится необходимостью для современных сетей?

26. Что представляет собой концепция SD-WAN, и какие преимущества она может предоставить организациям в управлении своими сетями?
27. Какие стандарты и топологии сетей используются в беспроводных сетях Wi-Fi 6 (802.11ax), и какие преимущества они приносят в сравнении с предыдущими версиями Wi-Fi?
28. Какие сетевые технологии и стандарты важны для успешной реализации интернета вещей (IoT), и какие вызовы могут возникнуть при создании сетей для подключенных устройств?
29. Какое значение имеет виртуализация сетей в современных сетях, и как она сочетается с концепцией Software-Defined Networking (SDN)?
30. Какие протоколы и методы обеспечивают безопасность сетей, особенно в контексте удаленного доступа и обмена конфиденциальной информацией в современных компьютерных сетях?
31. Какие инструменты и технологии используются для мониторинга и отладки сетевого взаимодействия в настольных приложениях?
32. Какие основные принципы взаимодействия настольных приложений с RESTful API, и какие HTTP-методы чаще всего используются для этой цели?
33. Какие практические задачи могут возникнуть при интеграции сетевых служб в настольные приложения, и как их можно решить?
34. В чем состоит роль форматов данных, таких как JSON и XML, в обмене информацией между настольными приложениями и сервером?
35. Какие архитектурные шаблоны, такие как клиент-сервер и peer-to-peer, могут быть применены при разработке настольных приложений сетевой инфраструктуры?
36. Какие практические советы вы бы дали разработчикам настольных приложений для оптимизации сетевого взаимодействия и улучшения производительности?
37. Что такое двухфакторная аутентификация, и как она может быть применена для обеспечения безопасности настольных приложений?
38. Какие основные меры безопасности можно применить для защиты данных пользователя в настольных приложениях?
39. Как обновления и патчи помогают в обеспечении безопасности настольных приложений, и почему их важно регулярно устанавливать?
40. Какие методы обеспечения безопасности сетевого взаимодействия влияют на безопасность настольных приложений при передаче данных через Интернет?
41. Какие основные принципы шифрования данных в настольных приложениях, и в каких случаях оно может быть полезным?
42. Какие меры обеспечения безопасности можно рекомендовать разработчикам приложений для защиты пользовательских данных от атак и утечек?
43. Какие основные компоненты входят в архитектуру сетевых серверов Cisco, и как они взаимодействуют между собой?
44. Какие шаги необходимо выполнить для начальной настройки сервера Cisco после его установки?
45. Какие методы конфигурации маршрутизации можно использовать на серверах Cisco, и какие основные настройки маршрутизации требуют внимания?
46. Какие меры безопасности можно применить на серверах Cisco для защиты сети и данных?
47. Как управлять пользователями и их учетными записями на серверах Cisco?
48. Какие инструменты и техники используются для мониторинга и диагностики состояния серверов Cisco?
49. Что такое горячее резервирование в контексте высокой доступности и как оно отличается от холодного резервирования?
50. Какие компоненты и сервисы обычно входят в состав высокодоступного кластера с Linux-серверами, и как они взаимодействуют между собой?

51. Какую роль играет протокол VRRP (Virtual Router Redundancy Protocol) в обеспечении высокой доступности сетевых устройств Cisco?
52. В чем заключается концепция "разделенного мозга" (split brain) в контексте кластеризации серверов, и какие меры предпринимаются для его предотвращения?
53. Какие метрики и инструменты используются для оценки эффективности и надежности высокодоступных систем?
54. Как можно реализовать механизм автоматического переключения между узлами кластера при обнаружении сбоя в работе одного из узлов?

6.2 Примеры тестовых заданий:

Тест № 1

Вариант 1

1. Какая из следующих служб является ответственной за преобразование доменных имен в IP-адреса?
 - a. DHCP
 - b. HTTP
 - c. DNS
 - d. FTP
2. Для чего служба DHCP (Dynamic Host Configuration Protocol) используется на сервере?
 - a. Распределение IP-адресов и сетевых настроек клиентам
 - b. Хранение веб-страниц на сервере
 - c. Маршрутизация сетевого трафика
 - d. Защита сервера от вредоносных программ
3. Какой из перечисленных протоколов обеспечивает безопасную передачу данных между клиентом и сервером, используя шифрование?
 - a. HTTP
 - b. DNS
 - c. HTTPS
 - d. FTP
4. Какой тип записи DNS используется для ассоциации IP-адреса с доменным именем?
 - a. CNAME
 - b. PTR
 - c. MX
 - d. A
5. Какая роль сервера DNS ответственна за перевод доменных имен в IP-адреса?
 - a. Роль прокси-сервера
 - b. Роль маршрутизатора
 - c. Роль ресурсного сервера
 - d. Роль авторитетного сервера
6. Какие из перечисленных служб работают на прикладном уровне модели OSI?
 - a. DHCP и DNS
 - b. FTP и HTTP
 - c. DNS и FTP
 - d. HTTP и DHCP
7. Какие преимущества предоставляет использование DNS-сервера с ролью кэширующего сервера?
 - a. Ускорен доступ к веб-сайтам
 - b. Распределение IP-адресов клиентам
 - c. Сохранение копий веб-страниц на сервере
 - d. Отслеживание сетевого трафика

8. Для чего служит запись PTR в DNS?
 - a. Для ассоциации IP-адреса с доменным именем
 - b. Для обратного преобразования IP-адреса в доменное имя
 - c. Для указания почтового сервера домена
 - d. Для установления защищенного соединения
9. Какие службы можно использовать для обеспечения безопасности сетевых соединений?
 - a. HTTPS и FTPS
 - b. HTTP и DNS
 - c. DHCP и FTP
 - d. SMTP и POP3
10. Какие из перечисленных протоколов используются для передачи файлов по сети?
 - a. HTTP и DNS
 - b. HTTPS и POP3
 - c. FTP и FTPS
 - d. DNS и DHCP
11. Какая роль DHCP-сервера включает в себя выделение IP-адресов клиентам?
 - a. Роль ресурсного сервера
 - b. Роль прокси-сервера
 - c. Роль авторитетного сервера
 - d. Роль маршрутизатора
12. Какие события можно найти в журнале событий Windows (Event Viewer)?
 - a. Ошибки приложений и события системного уровня
 - b. Ошибки DNS-сервера и DHCP-сервера
 - c. Попытки взлома сервера и атаки на сеть
 - d. Информация о подключенных клиентах
13. Какой протокол используется для передачи веб-страниц и данных между веб-сервером и клиентом?
 - a. FTP
 - b. HTTP
 - c. DNS
 - d. SMTP
14. Какие из перечисленных служб могут быть важными для обеспечения безопасности сети?
 - a. DHCP и HTTP
 - b. DNS и FTP
 - c. DNS и HTTPS
 - d. HTTP и FTP
15. Какая роль DNS-сервера предоставляет IP-адреса именам хостов в сети?
 - a. Роль прокси-сервера
 - b. Роль маршрутизатора
 - c. Роль авторитетного сервера
 - d. Роль кэширующего сервера

Ответы на тест № 1:

Вариант 1

- Вопрос 1: c
- Вопрос 2: a
- Вопрос 3: c
- Вопрос 4: d
- Вопрос 5: d
- Вопрос 6: a
- Вопрос 7: a
- Вопрос 8: b

Вопрос 9: a
Вопрос 10: c
Вопрос 11: a
Вопрос 12: a
Вопрос 13: b
Вопрос 14: c
Вопрос 15: d

Тест № 2

Вариант 1

1. Какая из перечисленных проблем может возникнуть, если вы создадите виртуальную машину без доступа к сети?
 - a. Проблема с диском
 - b. Проблема с процессами
 - c. Проблема с правами доступа
 - d. Проблема с сетью
2. Какая команда используется для диагностики сетевых проблем в Linux?
 - a. ``df``
 - b. ``du``
 - c. ``ifconfig``
 - d. ``chmod``
3. Какие команды позволяют узнать информацию о текущем состоянии системы и запущенных процессах?
 - a. ``top`` и ``ps``
 - b. ``ls`` и ``cd``
 - c. ``ping`` и ``traceroute``
 - d. ``chown`` и ``chmod``
4. Какие команды используются для изменения прав доступа к файлу или директории в Linux?
 - a. ``chown`` и ``chmod``
 - b. ``mv`` и ``cp``
 - c. ``grep`` и ``sed``
 - d. ``pwd`` и ``ls``
5. Что может быть причиной проблемы с диском в Linux?
 - a. Неправильные права доступа
 - b. Недостаточно места на диске
 - c. Проблемы с DNS
 - d. Ошибки в файле ``/etc/fstab``
6. Какие команды позволяют вам диагностировать проблему с процессами и завершить зависший процесс в Linux?
 - a. ``top`` и ``ps``
 - b. ``df`` и ``du``
 - c. ``ifconfig`` и ``netstat``
 - d. ``ping`` и ``traceroute``
7. Какая команда используется для выполнения DNS-запросов в Linux?
 - a. ``df``
 - b. ``nslookup``
 - c. ``ifconfig``
 - d. ``chown``
8. Какие типы прав доступа существуют в Linux?
 - a. Только "чтение" и "запись"
 - b. Только "чтение", "запись" и "исполнение"

- c. "Чтение", "запись" и "исполнение" для владельца, группы и остальных пользователей
 - d. Только "исполнение"
9. Какая команда используется для редактирования файла с настройками DNS в Linux?
- a. ``cat``
 - b. ``vi``
 - c. ``nslookup``
 - d. ``ping``
10. Как можно диагностировать и устранить проблему с загрузкой системы в Linux?
- a. Изменить настройки сети
 - b. Изменить настройки DNS
 - c. Воспользоваться командой ``grub`` для восстановления загрузки
 - d. Переустановить операционную систему
11. Какая команда используется для просмотра списка процессов, работающих в системе?
- a. ``top``
 - b. ``df``
 - c. ``ls``
 - d. ``ping``
12. Какие команды используются для установки нового программного обеспечения в Linux через командную строку?
- a. ``apt-get`` и ``yum``
 - b. ``mkdir`` и ``touch``
 - c. ``ls`` и ``cd``
 - d. ``grep`` и ``sed``
13. Как можно узнать, какие процессы используют наибольшее количество ресурсов в системе?
- a. С помощью команды ``ping``
 - b. С помощью команды ``df``
 - c. С помощью команды ``top``
 - d. С помощью команды ``nslookup``
14. Какие команды позволяют вам узнать, сколько свободного места осталось на диске в Linux?
- a. ``df`` и ``du``
 - b. ``ifconfig`` и ``netstat``
 - c. ``ping`` и ``traceroute``
 - d. ``chown`` и ``chmod``
15. Какая проблема может возникнуть, если DNS-серверы настроены неправильно в Linux?
- a. Проблема с сетью
 - b. Проблема с процессами
 - c. Проблема с правами доступа
 - d. Проблема с загрузкой

Ответы на тест № 2:

Вариант 1

- 1. Вопрос 1: d
- 2. Вопрос 2: c
- 3. Вопрос 3: a
- 4. Вопрос 4: a
- 5. Вопрос 5: b
- 6. Вопрос 6: a
- 7. Вопрос 7: b
- 8. Вопрос 8: c

- 9. Вопрос 9: b
- 10. Вопрос 10: c
- 11. Вопрос 11: a
- 12. Вопрос 12: a
- 13. Вопрос 13: a
- 14. Вопрос 14: a
- 15. Вопрос 15: a

Тест № 3

Вариант 1

1. Что включает в себя процесс анализа сетевой инфраструктуры для оптимизации?
 - a. Покупка нового оборудования
 - b. Изучение текущей инфраструктуры и выявление её сильных и слабых сторон
 - c. Установка дополнительных программ
 - d. Отключение сетевых устройств
2. Что означает масштабируемость в контексте сетевой инфраструктуры?
 - a. Возможность установки большего количества маршрутизаторов
 - b. Способность сети поддерживать высокую производительность при увеличении нагрузки
 - c. Способность увеличения размера сетевых интерфейсов
 - d. Возможность создания дополнительных сетей
3. Что такое аудит сетевой инфраструктуры?
 - a. Проверка качества сетевых устройств
 - b. Анализ текущей сетевой конфигурации и документации
 - c. Тестирование рабочих станций
 - d. Оценка цветовой схемы сети
4. Какие аспекты следует учитывать при оптимизации сетевой инфраструктуры?
 - a. Производительность, безопасность, масштабируемость и управляемость
 - b. Размер монитора на компьютерах
 - c. Количество принтеров в офисе
 - d. Скорость интернет-соединения
5. Какие инструменты можно использовать для мониторинга сетевой инфраструктуры?
 - a. Программа для редактирования текста
 - b. Система мониторинга сетевых устройств, SNMP-агенты, сетевые сканеры
 - c. Специализированное графическое программное обеспечение
 - d. Интернет-браузер
6. Что такое VLAN (Virtual LAN)?
 - a. Виртуальное сетевое устройство
 - b. Виртуальный коммутатор
 - c. Виртуальная локальная сеть, которая позволяет группировать устройства внутри сети независимо от физической топологии
 - d. Виртуальный сервер
7. Какие типы сетевых атак могут угрожать сетевой инфраструктуре?
 - a. Только атаки извне сети
 - b. Только атаки изнутри сети
 - c. Как атаки извне, так и изнутри сети
 - d. Только атаки на физическую инфраструктуру
8. Что такое QoS (Quality of Service) в сетевой инфраструктуре?
 - a. Качество обслуживания, которое определяет производительность серверов
 - b. Модель сетевой безопасности
 - c. Механизм, позволяющий управлять приоритетами и качеством обслуживания сетевого трафика

- d. Количество пользователей в сети
- 9. Какая из следующих мер является частью оптимизации сетевой инфраструктуры?
 - a. Изменение цвета кабельных проводов
 - b. Повышение скорости интернет-соединения
 - c. Внедрение мер безопасности
 - d. Увеличение количества сетевых устройств
- 10. Какие действия следует предпринимать при обнаружении узких мест в сетевой инфраструктуре?
 - a. Удалить все сетевые устройства
 - b. Оставить узкие места без изменений
 - c. Разработать и реализовать план для устранения узких мест
 - d. Покупать новые серверы

Вариант 2

- 1. Какие факторы следует учитывать при анализе сетевой инфраструктуры организации?
 - a. Только цвет кабелей
 - b. Производительность, безопасность, масштабируемость и управляемость
 - c. Размер офиса
 - d. Количество столов в офисе
- 2. Что означает масштабируемость сети?
 - a. Возможность увеличения количества бумаги в принтере
 - b. Способность сети поддерживать высокую производительность при увеличении нагрузки
 - c. Возможность увеличения размера сетевых кабелей
 - d. Способность сети работать без изменений
- 3. Какие действия включает в себя аудит сетевой инфраструктуры?
 - a. Покупка нового сетевого оборудования
 - b. Анализ текущей сетевой конфигурации и документации
 - c. Установка новых программ
 - d. Переустановка операционных систем
- 4. Что следует учитывать при оптимизации сетевой инфраструктуры?
 - a. Производительность, безопасность, масштабируемость и управляемость
 - b. Толщина стен в офисе
 - c. Количество розеток для подключения компьютеров
 - d. Марка кофемашины в офисе
- 5. Какие инструменты можно использовать для мониторинга сетевой инфраструктуры?
 - a. Чайник
 - b. Сетевые сканеры
 - c. Фотоаппарат
 - d. Клиентские сканеры
- 6. Что такое VLAN (Virtual LAN)?
 - a. Виртуальное сетевое устройство
 - b. Виртуальный коммутатор
 - c. Виртуальная локальная сеть, которая позволяет группировать устройства внутри сети независимо от физической топологии
 - d. Виртуальный рабочий стол
- 7. Какие типы сетевых атак могут угрожать сетевой инфраструктуре?
 - a. Только атаки снаружи сети
 - b. Только атаки изнутри сети
 - c. Как атаки снаружи, так и атаки изнутри сети
 - d. Только атаки на сотрудников офиса
- 8. Что означает QoS (Quality of Service) в сетевой инфраструктуре?

- a. Качество обслуживания, которое определяет производительность серверов
 - b. Модель сетевой безопасности
 - c. Механизм, позволяющий управлять приоритетами и качеством обслуживания сетевого трафика
 - d. Количество дней до оплаты интернет-счета
9. Какие действия следует предпринимать при обнаружении узких мест в сетевой инфраструктуре?
- a. Удалить все сетевые устройства
 - b. Оставить узкие места без изменений
 - c. Разработать и реализовать план для устранения узких мест
 - d. Купить больше офисной мебели
10. Какие факторы могут повлиять на производительность сети?
- a. Только количество кабельных проводов
 - b. Объем сетевого трафика, скорость передачи данных, конфигурация сетевых устройств
 - c. Цвет серверных стоек
 - d. Видеоинтерфейсы мониторов

Ответы на тест № 3:

Вариант 1

- 1. Вопрос 1: b
- 2. Вопрос 2: b
- 3. Вопрос 3: b
- 4. Вопрос 4: a
- 5. Вопрос 5: a
- 6. Вопрос 6: b
- 7. Вопрос 7: c
- 8. Вопрос 8: c
- 9. Вопрос 9: c
- 10. Вопрос 10: c

Вариант 2

- 1. Вопрос 1: b
- 2. Вопрос 2: b
- 3. Вопрос 3: b
- 4. Вопрос 4: a
- 5. Вопрос 5: b
- 6. Вопрос 6: c
- 7. Вопрос 7: c
- 8. Вопрос 8: c
- 9. Вопрос 9: c
- 10. Вопрос 10: b

Тест № 4

Вариант 1

1. Что такое ICMP, и для чего он используется при диагностике сетевых проблем?
- a. Протокол передачи данных
 - b. Протокол управления передачей данных
 - c. Протокол маршрутизации
 - d. Протокол управления сетью (SNMP)
2. Какая команда Cisco IOS используется для проверки доступности удаленного устройства по IP-адресу?

- a. trace
 - b. ping
 - c. connect
 - d. ssh
3. Какие методы обеспечивают высокую доступность в сети Cisco?
- a. RIP и OSPF
 - b. ICMP и Telnet
 - c. HSRP и VRRP
 - d. DHCP и DNS
4. Что представляет собой протокол HSRP, и какие узлы в сети его используют?
- a. Протокол динамической маршрутизации
 - b. Протокол для работы с ARP
 - c. Протокол для обеспечения высокой доступности
 - d. Протокол для шифрования данных
5. Какой протокол используется для мониторинга и диагностики сетевых устройств Cisco?
- a. HTTP
 - b. SNMP
 - c. ICMP
 - d. SMTP
6. Какой протокол обеспечивает безопасное удаленное управление устройствами Cisco?
- a. FTP
 - b. Telnet
 - c. SSH
 - d. DNS
7. Что представляет собой "разделенный мозг" (split brain) в контексте кластеризации серверов?
- a. Две половины мозга
 - b. Разделенное ядро ОС
 - c. Две независимые части кластера
 - d. Сетевой сбой
8. Какие шаги следует предпринять при обнаружении сетевых сбоев для быстрого восстановления?
- a. Выключить сервер
 - b. Переустановить операционную систему
 - c. Анализировать причины сбоя и восстанавливать соединение
 - d. Позвонить в поддержку
9. Какие инструменты и технологии используются для анализа производительности сетевых устройств Cisco?
- a. Телеметрия и анализаторы сети
 - b. Фотоаппараты и видеорекамеры
 - c. Сканеры и принтеры
 - d. Клавиатура и мышь
10. Какие протоколы обеспечивают быстрое восстановление после сбоев в работе высокодоступных кластеров серверов Cisco?
- a. HTTP и FTP
 - b. HSRP и VRRP
 - c. BGP и OSPF
 - d. SMTP и POP3

Вариант 2

1. Что такое ICMP, и для чего он используется при диагностике сетевых проблем?
- a. Протокол передачи данных
 - b. Протокол управления передачей данных

- c. Протокол маршрутизации
 - d. Протокол управления сетью (SNMP)
2. Какая команда Cisco IOS используется для проверки доступности удаленного устройства по IP-адресу?
- a. trace
 - b. ping
 - c. connect
 - d. ssh
3. Какие методы обеспечивают высокую доступность в сети Cisco?
- a. RIP и OSPF
 - b. ICMP и Telnet
 - c. HSRP и VRRP
 - d. DHCP и DNS
4. Что представляет собой протокол HSRP, и какие узлы в сети его используют?
- a. Протокол динамической маршрутизации
 - b. Протокол для работы с ARP
 - c. Протокол для обеспечения высокой доступности
 - d. Протокол для шифрования данных
5. Какой протокол используется для мониторинга и диагностики сетевых устройств Cisco?
- a. HTTP
 - b. SNMP
 - c. ICMP
 - d. SMTP
6. Какой протокол обеспечивает безопасное удаленное управление устройствами Cisco?
- a. FTP
 - b. Telnet
 - c. SSH
 - d. DNS
7. Что представляет собой "разделенный мозг" (split brain) в контексте кластеризации серверов?
- a. Две половины мозга
 - b. Разделенное ядро ОС
 - c. Две независимые части кластера
 - d. Сетевой сбой
8. Какие шаги следует предпринять при обнаружении сетевых сбоев для быстрого восстановления?
- a. Выключить сервер
 - b. Переустановить операционную систему
 - c. Анализировать причины сбоя и восстанавливать соединение
 - d. Позвонить в поддержку
9. Какие инструменты и технологии используются для анализа производительности сетевых устройств Cisco?
- a. Телеметрия и анализаторы сети
 - b. Фотоаппараты и видеокамеры
 - c. Сканеры и принтеры
 - d. Клавиатура и мышь
10. Какие протоколы обеспечивают быстрое восстановление после сбоев в работе высокодоступных кластеров серверов Cisco?
- a. HTTP и FTP
 - b. HSRP и VRRP
 - c. BGP и OSPF
 - d. SMTP и POP3

Ответы на тест № 4:

Вариант 1

1. Вопрос 1: с
2. Вопрос 2: b
3. Вопрос 3: с
4. Вопрос 4: с
5. Вопрос 5: b
6. Вопрос 6: с
7. Вопрос 7: с
8. Вопрос 8: с
9. Вопрос 9: a
10. Вопрос 10: b

Вариант 2

1. Вопрос 1: с
2. Вопрос 2: b
3. Вопрос 3: с
4. Вопрос 4: с
5. Вопрос 5: b
6. Вопрос 6: с
7. Вопрос 7: с
8. Вопрос 8: с
9. Вопрос 9: a
10. Вопрос 10: b

6.3 Лабораторные работы:

Лабораторная работа № 1: Установка Windows Server 2012 R2

Цель задания: Освоить процесс установки Windows Server 2012 R2 на физическое или виртуальное оборудование.

Инструкции:

1. **Выбор оборудования:** В зависимости от доступного оборудования и доступных ресурсов, выберите одну из следующих опций:
 - Установите Windows Server 2012 R2 на виртуальную машину, используя программное обеспечение виртуализации, такое как VirtualBox, VMware Workstation или Hyper-V.
 - Установите Windows Server 2012 R2 на физический сервер, если у вас есть физическое оборудование для этой цели.
2. **Подготовка ISO-образа:** Загрузите ISO-образ операционной системы Windows Server 2012 R2 с официального сайта Microsoft или используйте предоставленный образ.
3. **Установка операционной системы:**
 - В случае виртуальной машины: Создайте новую виртуальную машину с соответствующими параметрами (количество ядер процессора, объем оперативной памяти и т. д.). Установите операционную систему с использованием загруженного ISO-образа.
 - В случае физического сервера: Подключите загрузочный носитель с ISO-образом операционной системы к серверу и запустите установку.
4. **Конфигурация установки:**
 - Выберите язык и региональные настройки.
 - Укажите ключ продукта (если требуется).
 - Выберите тип установки (стандартная или пользовательская).
5. **Диск и разделы:**

- Укажите диск и раздел, на который будет установлена операционная система.
 - Выберите опции форматирования и файловой системы.
6. **Имя компьютера и пароль администратора:**
- Укажите имя сервера.
 - Создайте и подтвердите пароль администратора.
7. **Установка и ожидание:**
- Дождитесь завершения установки операционной системы.
 - После завершения установки выполните первоначальную настройку, включая выбор ролей сервера, настройку сетевых параметров и обновление системы через Windows Update (если это необходимо).
8. **Проверка работы:**
- Убедитесь, что сервер успешно загрузился в операционную систему.
 - Попробуйте подключиться к серверу удаленно, используя службу удаленного рабочего стола (RDP), чтобы убедиться, что сервер доступен.
9. **Документация:**
- Составьте краткий отчет о вашей установке Windows Server 2012 R2, включая шаги, которые вы выполнили, и любые проблемы, с которыми вы столкнулись.

Замечание: Эта лабораторная работа поможет студентам овладеть процессом установки Windows Server 2012 R2 на физическое или виртуальное оборудование и настроить базовую конфигурацию операционной системы.

Время выполнения – 90 минут.

Лабораторная работа № 2: Резервное копирование и восстановление данных на сервере Windows Server 2012 R2

Цель работы: Освоить процессы резервного копирования и восстановления данных на сервере под управлением Windows Server 2012 R2.

Необходимое оборудование и программное обеспечение:

1. Сервер с установленной операционной системой Windows Server 2012 R2.
2. Виртуальная машина (VM) с клиентской операционной системой (например, Windows 10) для тестирования восстановления.
3. Программа для создания резервных копий (например, Windows Server Backup).
4. Доступ к сетевым ресурсам (файлам и папкам), которые будут резервироваться.

Шаги выполнения:

1. *Настройка среды:*
 - Убедитесь, что сервер и клиентская VM находятся в одной сети и имеют свободное место на диске для хранения резервных копий.
2. *Создание резервной копии:*
 - Используя программу для создания резервных копий (например, Windows Server Backup), настройте резервное копирование выбранных данных на сервере.
 - Укажите расписание резервного копирования (например, ежедневное, еженедельное).
3. *Запуск резервного копирования:*
 - Запустите первую резервную копию данных на сервере согласно расписанию.
4. *Проверка резервной копии:*
 - Убедитесь, что резервная копия успешно завершена и данные сохранены.
5. *Симуляция ситуации восстановления:*
 - Создайте сценарий, который потребует восстановления данных (например, случайное удаление важных файлов или папок на сервере).
6. *Восстановление данных:*

- Используя программу для восстановления данных (например, Windows Server Backup), выполните процедуру восстановления данных согласно созданному сценарию.
7. *Проверка восстановленных данных:*
 - Убедитесь, что данные были успешно восстановлены и доступны на сервере.
 8. *Документация и отчет:*
 - Составьте отчет, включающий информацию о настройке резервного копирования, процессе восстановления и результате проверки восстановленных данных.
 9. *Обсуждение и анализ:*
 - Проведите обсуждение процесса резервного копирования и восстановления данных, выявите потенциальные проблемы и рекомендации по улучшению процесса.

Замечание: Лабораторная работа позволяет студентам на практике ознакомиться с процессами резервного копирования и восстановления данных на сервере Windows Server 2012 R2. Это важный аспект администрирования серверов и обеспечения безопасности данных.

Время выполнения – 90 минут.

Лабораторная работа № 3: Мониторинг и диагностика состояния сервера в Windows Server 2012 R2

Цель задания: Освоить различные методы мониторинга и диагностики состояния сервера на платформе Windows Server 2012 R2.

Инструкции:

1. **Performance Monitor (Performance Counters):**
 - Откройте Performance Monitor на вашем сервере.
 - Выберите несколько счетчиков производительности (Performance Counters), таких как процент загрузки процессора, использование памяти и использование дискового пространства.
 - Создайте логирование для этих счетчиков и настройте его на запись данных каждые 5 минут в течение часа.
 - Анализируйте полученные данные и определите, есть ли какие-либо аномалии или узкие места в производительности сервера.
2. **Службы и журналы событий (Event Logs):**
 - Просмотрите журнал событий (Event Viewer) на сервере.
 - Найдите и проанализируйте несколько записей журнала, связанных с событиями произошедшими в последние 24 часа, такие как ошибки приложений, события системного уровня и важные события безопасности.
 - Определите, были ли какие-либо проблемы или ненормальные события на сервере.
3. **Диагностические инструменты (Diagnostic Tools):**
 - Запустите инструмент диагностики сервера (Server Diagnostic Tools) в Windows Server 2012 R2.
 - Выполните базовую диагностику состояния сервера с использованием этого инструмента.
 - Проанализируйте результаты и определите, есть ли какие-либо рекомендации по улучшению состояния сервера.
4. **Утилиты командной строки:**
 - Откройте командную строку (Command Prompt) с правами администратора.
 - Запустите утилиту Tasklist для просмотра активных процессов на сервере.
 - Выполните команду Netstat для просмотра активных сетевых соединений.

- Поделитесь выводом этих команд и опишите, какие процессы и сетевые соединения активны на сервере.
5. **Мониторинг сети (Network Monitoring):**
- Загрузите и установите инструмент мониторинга сети, такой как Wireshark, на ваш сервер.
 - Запустите инструмент и начните запись сетевого трафика на сервере.
 - Проанализируйте записанные данные и определите, какие сетевые запросы и ответы были зафиксированы.
6. **Отчет:**
- Создайте отчет, включающий результаты всех проведенных шагов.
 - Опишите любые аномалии или проблемы, которые были обнаружены в процессе мониторинга и диагностики сервера.
 - Предложите рекомендации по улучшению производительности и стабильности сервера.

Замечание: Эта лабораторная работа позволит студентам ознакомиться с различными методами мониторинга и диагностики сервера в Windows Server 2012 R2 и развить навыки администрирования.

Время выполнения – 90 минут.

Лабораторная работа № 4: Мониторинг и диагностика состояния сервера в Windows Server 2012 R2

Цель задания: Продолжить изучение методов мониторинга и диагностики состояния сервера в операционной системе Windows Server 2012 R2.

Инструкции:

Часть 1: Мониторинг ресурсов сервера

1. Использование Resource Monitor:

- Откройте Resource Monitor на сервере (можно найти в "Диспетчере задач" в разделе "Вкладка "Производительность").
- Оцените использование CPU, памяти, дискового пространства и сетевого трафика на сервере в режиме реального времени.
- Запишите наблюдения о текущей производительности сервера.

2. Применение PerfMon (Performance Monitor):

- Запустите PerfMon (Performance Monitor).
- Создайте новый набор данных (Data Collector Set) для мониторинга производительности.
- Настройте счетчики производительности для мониторинга CPU, памяти, дискового ввода/вывода и сетевых интерфейсов.
- Запустите сбор данных на протяжении 15 минут.
- Проанализируйте результаты и определите, есть ли какие-либо узкие места или проблемы производительности.

Часть 2: Мониторинг событий и журналов

3. Анализ событий Windows:

- Перейдите в "Диспетчер событий" (Event Viewer) на сервере.
- Проанализируйте записи в журналах событий Windows, таких как "Журнал системы" и "Журнал безопасности".
- Найдите и проанализируйте любые критические или важные события, которые могли возникнуть в последние 24 часа.

Часть 3: Дополнительные задачи

4. Использование PowerShell:

- Откройте PowerShell на сервере.
- Используйте командлеты PowerShell для получения информации о текущем

- состоянии служб, сетевых подключениях и ресурсах сервера.
- Создайте скрипт PowerShell для автоматического мониторинга и регистрации состояния сервера.

5. Использование дополнительных инструментов:

- Исследуйте и опишите какой-либо дополнительный инструмент или утилиту, которая может использоваться для мониторинга и диагностики сервера в Windows Server 2012 R2.
- Поделитесь информацией о том, как этот инструмент может быть полезен при администрировании сервера.

Часть 4: Отчет

6. Составление отчета:

- Создайте подробный отчет о результатах вашего мониторинга и диагностики сервера.
- Укажите любые обнаруженные проблемы или узкие места в производительности.
- Дайте рекомендации по оптимизации сервера и улучшению его производительности и стабильности.

Замечание: Эта лабораторная работа позволит студентам углубить свои знания о методах мониторинга и диагностики состояния сервера в Windows Server 2012 R2 и развить навыки администрирования и решения проблем.

Время выполнения – 90 минут.

Лабораторная работа № 5: Диагностика и устранение сетевых проблем на клиентском компьютере

Цель работы: Научить студентов диагностировать и решать типичные сетевые проблемы на клиентских компьютерах, включая настройку сетевых параметров и использование инструментов диагностики.

Необходимое оборудование и программное обеспечение:

1. Компьютеры с установленной операционной системой Windows (или другой по выбору).
2. Сетевое оборудование (маршрутизатор, коммутатор, кабели).
3. Интернет-соединение (опционально).
4. Программы для диагностики сети, такие как ping, ipconfig, tracert.

Шаги выполнения:

1. *Настройка сетевых параметров:*
 - Студенты должны настроить сетевые параметры (IP-адрес, маску подсети, шлюз, DNS) на клиентских компьютерах.
 - Задача может включать создание статической и динамической (через DHCP) конфигурации.
2. *Диагностика сетевых проблем:*
 - Проведите симуляцию типичных сетевых проблем, таких как отсутствие подключения к интернету, недоступность определенного веб-сайта и т. д.
 - Студенты должны использовать инструменты диагностики, например, ping, ipconfig, tracert, для выявления и анализа проблемы.
3. *Устранение сетевых проблем:*
 - Студенты должны разработать план устранения сетевой проблемы на основе результатов диагностики.
 - Примените необходимые действия, чтобы восстановить работоспособность сети или интернет-соединения.
4. *Отчет и анализ:*
 - Каждый студент должен составить отчет, описывающий выявленную

- проблему, примененные методы диагностики и действия по устранению.
- Сделайте выводы о том, какие знания и навыки были применены при решении проблемы.

5. *Обсуждение:*

- Проведите обсуждение результатов лабораторной работы, обменяйтесь опытом в решении сетевых проблем.
- Обсудите возможные варианты улучшения диагностики и решения сетевых проблем.

Замечание: Эта лабораторная работа может быть адаптирована под конкретные потребности и уровень подготовки студентов. Важно, чтобы студенты получили практический опыт в настройке сетевых параметров, диагностике и устранении сетевых проблем на клиентских компьютерах.

Время выполнения – 90 минут.

Лабораторная работа № 6: Управление групповой политикой в Windows

Цель работы: Изучить процесс установки, настройки и управления групповой политикой в операционной системе Windows.

Задачи:

1. Создать новую групповую политику в Active Directory.
2. Назначить групповую политику для определенной группы пользователей.
3. Настроить различные параметры политики, такие как настройки безопасности, рабочего стола и сетевых параметров.
4. Протестировать применение групповой политики на клиентской системе.

Шаги выполнения:

Шаг 1: Создание групповой политики:

1. Откройте "Групповую политику управления" на контроллере домена Windows.
2. Создайте новую групповую политику с именем "Лабораторная политика".
3. Настройте различные параметры политики, такие как пароли, разрешения и настройки рабочего стола.

Шаг 2: Назначение политики группе пользователей:

1. Создайте новую группу пользователей с именем "Лабораторная группа".
2. Назначьте групповую политику "Лабораторная политика" для этой группы.

Шаг 3: Настройка параметров политики:

1. Внесите изменения в политику, такие как установка сложности паролей и блокировка рабочего стола после периода неактивности.
2. Настройте сетевые параметры, например, настройки прокси-сервера и безопасности сети.

Шаг 4: Тестирование применения политики:

1. Запустите клиентскую систему и войдите в нее с учетной записью пользователя из группы "Лабораторная группа".
2. Убедитесь, что настройки политики успешно применяются на клиентской системе.

Замечание: В результате выполнения лабораторной работы вы изучили процесс установки, настройки и управления групповой политикой в операционной системе Windows. Вы также научились создавать и назначать групповую политику для определенных групп пользователей, а также настраивать различные параметры политики для обеспечения безопасности и эффективности настольных приложений.

Время выполнения – 90 минут.

Лабораторная работа № 7:

Цель работы: Изучить процесс начальной настройки и управления сетевыми устройствами

Cisco для обеспечения правильной работы сети.

Задачи:

1. Подключение к маршрутизатору и коммутатору Cisco.
2. Начальная настройка базовых параметров устройств.
3. Создание виртуальных LAN (VLAN) на коммутаторе.
4. Настройка маршрутизации между VLAN на маршрутизаторе.
5. Настройка списков доступа (ACL) для контроля трафика.
6. Тестирование и проверка конфигурации устройств.

Шаги выполнения:

Шаг 1: Подключение к устройствам Cisco:

1. Подключите компьютер к консольному порту маршрутизатора Cisco и коммутатора Cisco с помощью консольного кабеля.
2. Запустите программу терминала для доступа к устройствам через консоль.

Шаг 2: Начальная настройка устройств:

1. Выполните начальную настройку маршрутизатора, включая настройку имени устройства и пароля для доступа.
2. Выполните начальную настройку коммутатора, включая установку пароля для входа.

Шаг 3: Создание VLAN на коммутаторе:

1. Создайте несколько виртуальных LAN (VLAN) на коммутаторе и назначьте порты к определенным VLAN.

Шаг 4: Настройка маршрутизации между VLAN на маршрутизаторе:

1. Настройте маршрутизатор для обеспечения маршрутизации между VLAN и доступа к другим сетям.

Шаг 5: Настройка списков доступа (ACL) :

1. Создайте списки доступа (ACL) на маршрутизаторе для ограничения трафика между VLAN.
2. Настройте правила ACL для контроля трафика.

Шаг 6: Тестирование и проверка:

1. Проверьте работу сети, отправляя пакеты между устройствами и проверяя выполнение настроек VLAN и ACL.
2. Завершите лабораторную работу, удостоверившись, что устройства настроены правильно и сеть функционирует корректно.

Замечание: В результате выполнения лабораторной работы студенты изучат основы настройки и управления сетевыми устройствами Cisco, включая маршрутизаторы и коммутаторы. Они также научатся создавать виртуальные LAN (VLAN), настраивать маршрутизацию между VLAN и применять списки доступа (ACL) для контроля трафика в сети.