ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Петербургский государственный университет путей сообщения Императора Александра I»
(ФГБОУ ВО ПГУПС)

Петрозаводский филиал ПГУПС

ОДОБРЕНО
на заседании цикловой комиссии
протокол № 11 от 23.06.2017
Председатель цикловой комиссии:
_____ (Камашев)

УТВЕРЖДАЮ
Начальник УМО
_____ А.В. Калько
«23» 06 2017г.

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по организации и проведению практических занятий и лабораторных работ

По МДК: МДК.03.01.Эксплуатация объектов сетевой инфраструктуры

Специальность: 09.02.02 Компьютерные сети

Выполнил: преподаватель ПФ ПГУПС, Лятти Алексей Александрович

2017г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические указания по организации и проведению лабораторных работ и практических занятий разработаны в соответствии с рабочей программой междисциплинарного курса МДК.03.01. Эксплуатация объектов сетевой инфраструктуры и предназначено для выполнения практических занятий и лабораторных работ обучающимися.

Практические занятия и лабораторные работы по междисциплинарному курсу направлены на усвоение знаний, освоение умений и формирование элементов общих компетенций, предусмотренных рабочей программой учебной дисциплины.

В результате освоения учебной дисциплины обучающийся должен

уметь:

выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;

использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;

осуществлять диагностику и поиск неисправностей технических средств;

выполнять действия по устранению неисправностей в части, касающейся полномочий техника;

тестировать кабели и коммуникационные устройства;

выполнять замену расходных материалов и мелкий ремонт периферийного оборудования;

правильно оформлять техническуюдокументацию;

наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;

устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;

знать:

архитектуру и функции систем управления сетями, стандарты систем управления;

задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;

средства мониторинга и анализа локальных сетей;

классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;

правила эксплуатации технических средств сетевой инфраструктуры;

расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;

методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;

основные понятия информационных систем, жизненный цикл, проблемы обеспечения технологической безопасности информационных систем, требования к архитектуре информационных систем и ихкомпонентам для обеспечения безопасности функционирования, оперативные методы повышения безопасности функционирования программных средств и баз данных;

основные требования к средствам и видам тестирования для определения технологической безопасности информационных систем.

В результате освоения междисциплинарного курса происходит поэтапное формирование элементов общих и профессиональных компетенций:

ПК 3.1. Устанавливать, настраивать, эксплуатировать и обслуживать технические и программно-аппаратные средства компьютерных сетей.

ПК 3.2. Проводить профилактические работы на объектах сетевой инфраструктуры и рабочих станциях.

ПК 3.3. Эксплуатация сетевых конфигураций.

ПК 3.4. Участвовать в разработке схемы послеаварийного восстановления работоспособности компьютерной сети, выполнять восстановление и резервное копирование информации.

ПК 3.5. Организовывать инвентаризацию технических средств сетевой инфраструктуры, осуществлять контроль оборудования после его ремонта.

ПК 3.6. Выполнять замену расходных материалов и мелкий ремонт периферийного оборудования, определять устаревшее оборудование и программные средства сетевой инфраструктуры.

ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.

ОК 2. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.

ОК 3. Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность.

ОК 4. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.

ОК 5. Использовать информационно-коммуникационные технологии в профессиональной деятельности.

ОК 6. Работать в коллективе и в команде, эффективно общаться с коллегами, руководством, потребителями.

ОК 7. Брать на себя ответственность за работу членов команды (подчиненных), за результат выполнения заданий.

ОК 8. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.

ОК 9. Ориентироваться в условиях частой смены технологий в профессиональной деятельности.

Рабочей программой предусмотрено выполнение обучающимися практических занятий, включая, как обязательный компонент практические задания с использованием персонального компьютера.

Распределение результатов освоения учебного материала в ходе выполнения лабораторных работ и заданий на практических занятиях происходит в соответствии с таблицей 1.

Таблица 1 – Распределение результатов освоения учебного материала

Контрольно-оценочные мероприятия	Кол-во часов	результаты		Поэтапно формируемые элементы общих и профессиональных компетенций
		Усвоенные знания	Освоенные умения	
Практическое занятие №1 Оформление технической документации, правила оформления документов.	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;	правильно оформлять техническую документацию;	ОК1-9, ПК 3.5.
Практическое занятие №2 Разработка проекта компьютерной сети организации.	8	архитектуру и функции систем управления сетями, стандарты систем управления;	правильно оформлять техническую документацию;	ОК1-9, ПК 3.3.
Лабораторная работа №1 Установка штекеров RJ45 на кабель UTP5 по стандартам A, B, с подключением телефонной линии, с питанием по витой паре.	4	правила эксплуатации технических средств сетевой инфраструктуры;	тестировать кабели и коммуникационные устройства;	ОК1-9, ПК 3.1.ПК 3.2.
Лабораторная работа №2 Настройка сетевых интерфейсов в ОС Windows	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	ОК1-9, ПК 3.1. ПК 3.3.
Лабораторная работа №3 Настройка сетевых интерфейсов в ОС Linux	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	ОК1-9, ПК 3.1. ПК 3.3.
Лабораторная работа №4 Установка и настройка коммутатора Cisco	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	тестировать кабели и коммуникационные устройства;	ОК1-9, ПК 3.1.ПК 3.3.
Лабораторная работа №5 Установка и настройка маршрутизатора Cisco	4	задачи управления: анализ производительности и	тестировать кабели и коммуникационные	ОК1-9, ПК 3.1. ПК 3.3.

		надежности, управление безопасностью, учет трафика, управление конфигурацией;	устройства;	
Лабораторная работа №6 Разбиение сети на подсети	4	правила эксплуатации технических средств сетевой инфраструктуры;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1. ПК 3.3.
Лабораторная работа №7 Управление учетными записями и правами доступа в MicrosoftWindows	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1.
Лабораторная работа №8 Управление сетевыми службами в MicrosoftWindows	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1.
Лабораторная работа №9 Установка и настройка HTTP-клиента и HTTP-сервера, FTP-клиента и FTP-сервера.	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1.
Лабораторная работа №10 Настройка и использование средств удаленного администрирования и удаленного доступа.	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией; средства мониторинга и анализа локальных сетей;	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	ОК1-9, ПК 3.1.
Лабораторная работа №11 Установка и настройка сетевых служб в UNIX, управление пользователями и правами доступа.	4	задачи управления: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать	ОК1-9, ПК 3.1.

			антивирусную защиту;	
Лабораторная работа №12 Диагностика и устранение неисправностей пассивного оборудования компьютерных сетей	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	осуществлять диагностику и поиск неисправностей технических средств;	ОК1-9, ПК 3.1.ПК 3.2.
Лабораторная работа №13 Диагностика и устранение неисправностей активного оборудования компьютерных сетей	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	осуществлять диагностику и поиск неисправностей технических средств;	ОК1-9, ПК 3.1.ПК 3.2.
Лабораторная работа №14 Применение программных средств диагностики компьютерной сети.	2	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	выполнять мониторинг и анализ работы локальной сети с помощью программно-аппаратных средств;	ОК1-9, ПК 3.1.ПК 3.2.
Лабораторная работа №15 Применение Плана действий восстановления работоспособности в реальной сети организации.	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры;	ОК1-9, ПК 3.1.ПК 3.2.ПК 3.5.
Лабораторная работа №16 Диагностика компьютерных комплексов и систем помощью диагностической программы AIDA 64.	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	осуществлять диагностику и поиск неисправностей технических средств;	ОК1-9, ПК 3.1.ПК 3.2.ПК 3.6.
Лабораторная работа №17 Техническое обслуживание	4	классификацию регламентов, порядок	осуществлять диагностику и	ОК1-9, ПК 3.1.ПК

клавиатуры и манипулятора типа мышь.		технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	поиск неисправностей технических средств;	3.2.ПК 3.6.
Лабораторная работа №18 Техническое обслуживание лазерных принтеров и их картриджей.	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ;	осуществлять диагностику и поиск неисправностей технических средств; выполнять действия по устранению неисправностей в части, касающейся полномочий техника; выполнять замену расходных материалов и мелкий ремонт периферийного оборудования	ОК1-9, ПК 3.1.ПК 3.2.ПК 3.5.ПК 3.6.
Лабораторная работа №19 Диагностика и устранение неисправностей в программном обеспечении.	4	классификацию регламентов, порядок технических осмотров, проверок и профилактических работ; расширение структуры, методы и средства диагностики неисправностей технических средств и сетевой структуры;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1.ПК 3.2.
Лабораторная работа №20 Работа с антивирусными пакетами.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №21 Создание хранилища данных на основе RAID.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию,	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.

		способы резервного копирования данных, принципы работы хранилищ данных;		
Лабораторная работа №22 Изучение возможностей архиваторов на примере pkzip, pkunzip, arj, WinZip, 7Zip.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №23 Изучение возможностей программного обеспечения резервного копирования на примере MicrosoftNtbackup, CobianBackup и AscompBackupMaker.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №24 Создание точек восстановления Windows в ручном и автоматическом режимах. Восстановление Windows. Клонирование и восстановление ОС на примере DiskImage, HDClone, ODIN.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	использовать схемы послеаварийного восстановления работоспособности сети, эксплуатировать технические средства сетевой инфраструктуры; наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №25 Установка обновлений ПО и ОС с сайта производителя, автоматизация обновления, создание сервера обновлений.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1.ПК 3.4.

Лабораторная работа №26 Изучение журналов и оповещений Windows и Unix, настройка службы аудита Windows.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №27 Управление сетями на основе протокола SNMP.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №28 Анализ сетевого трафика средствами Сетевого монитора	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1. ПК 3.4.
Лабораторная работа №29 Установка и использование программы Wireshark.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	устанавливать, тестировать и эксплуатировать информационные системы, согласно технической документации, обеспечивать антивирусную защиту;	ОК1-9, ПК 3.1. ПК 3.4.

Лабораторная работа №30 Мониторинг сетевой активности и производительности.	4	методы устранения неисправностей в технических средствах, схемы послеаварийного восстановления работоспособности сети, техническую и проектную документацию, способы резервного копирования данных, принципы работы хранилищ данных;	наблюдать за трафиком, выполнять операции резервного копирования и восстановления данных;	ОК1-9, ПК 3.1. ПК 3.4.

Содержание практических занятий и лабораторных работ охватывает весь круг умений и компетенций, на формирование которых направленМДК.

КРИТЕРИИ ОЦЕНИВАНИЯ ПРАКТИЧЕСКИХ РАБОТ

При оценке освоенных умений при выполнении практических работ применяется дихотомическая шкала оценивания.

Оценивание практических занятий/лабораторных работ производится в соответствии со следующими нормативными актами:

- Положение о текущем контроле успеваемости и промежуточной аттестации обучающихся;

- Положение о планировании, организации и проведении лабораторных работ и практических занятий.

Практическое задание № 1

Оформление технической документации, правила оформления документов.

Цели работы: научиться оформлять техническую документацию согласно действующих стандартов.

Теоретическая часть

Оформление технической документации (набора документов) — необходимое условие проектирования, создания и эксплуатации любых технических объектов: зданий, строений, сооружений, промышленных товаров, оборудования, программного обеспечения.

Для оформления технической документации необходимо пройти процедуру инвентаризации (технического учета), по результатам которой объекту исследования присваиваются определенные, выделяющие его из ряда аналогов свойства и характеристики, официально утверждаемые в соответствующем документе: паспорте, технической литературе, руководстве по эксплуатации.

Ход работы

1. Создание паспорта кабинета.

1.1.Назначение кабинета.

1.2.Технические характеристики кабинета.

1.3.Перечень оборудования в кабинете.

1.4.План кабинета.

Разработайте план кабинета в MsVisio.

2. Распечатайте план кабинета и сдайте преподавателю.
3. Вывод.

Практическое занятие №2

Разработка проекта компьютерной сети организации.

Цель:закрепить и систематизировать знания по принципам проектирования локальных сетей; получить навыки конфигурирования локальной компьютерной сети в зависимости от возлагаемых на нее функций, создать план-проект локальной вычислительной сети организации или предприятия.

Занятие выполнено в виде деловой игры.

ПОДГОТОВКА К ИГРЕ

Студенты группы распределяется на команды по 5 человек. Команда проекта состоит из «Руководителя проекта», «Экономиста», «ИТ- специалиста», «Монтажника компьютерной сети», «Техника по компьютерным сетям».

1. «Руководитель проекта». В его обязанности входит:

- создает планы работ;
- координирует работу команды проекта;
- принимает решения по оперативным вопросам;
- ставит задачи участникам команды проекта в соответствии с утвержденным планом;
- контролирует работу каждого члена команды.

2. «Экономист» - специалист, выполняющий технико-экономическое обоснование проекта компьютерной сети, т.е. выполняет расчет примерной стоимости реализации проекта и его внедрения в организации.

3. «ИТ-специалист» – выполняет работы связанные с подбором оборудования для проектируемой сети, а так же составляет сметы затрат на реализацию проекта компьютерной сети. В его обязанности входит:

- составление технического задания на закупку оборудования для организации;

– рациональное размещение оборудования (в том числе и сетевого) и офисной техники (работа выполняется совместно с «Техником по компьютерным сетям»);

– составление смету на закупку компьютеров и офисной техники;

– составление сметы на закупку сетевого оборудования и материалов на организацию компьютерной сети (возможны консультации «Монтажника компьютерной сети»).

4. «Монтажник компьютерной сети»,его задачей являетсярасчет стоимости монтажных работ в соответствии с планом размещения оборудования, дальнейшая прокладка кабельных систем и настройка оборудования (при реализации проекта), так же он может осуществлять консультации «Техника по компьютерным сетям» и «ИТ-специалиста» касательно размещения оборудования, для минимизации затрат при реализации проекта.

5. «Техник по компьютерным сетям», его задачей является выбор необходимых технологий проектирования и дополнительных критериев работы компьютерной сети. К его основным функциям относятся:

– выбор топологии и технологий реализации компьютерной сети, методов доступа к каналам связи и типа среды передачи данных;

– разработка требований к расширяемости и масштабируемости сети, безопасности и надежности оборудования и компьютерной сети в целом;

– рациональное размещение сетевого оборудования и офисной техники (работа выполняется совместно с «ИТ-специалистом»);

– составление перспектив развития вычислительной сети и рассмотрение технических средств позволяющих повысить надежность и время безотказной работы сетевого оборудования и сети в целом.

После распределения участников по ролям, преподаватель-огранизатор объясняет правила и цели игры.

РАЗДАТОЧНЫЙ МАТЕРИАЛ И ИСПОЛЬЗУЕМЫЕ СРЕДСТВА

Каждая команда получает набор инструкционных карт, далее эти карты раздаются участникам команды в соответствии с, уже распределенными, проектными ролями.

Для проведения деловой игры необходимы следующие средства:

1. Персональный компьютер или ноутбук с возможностью доступа в Интернет (для каждого члена проекта);
2. Программный продукт MSOfficeVisio 2007/2010/2013 или систему автоматизированного проектирования Компас 3d;
3. Программный продукт MS Office Word 2007/2010/2013 Professional;
4. Программный продукт MS Office Power Point 2007/2010/2013 Professional;
5. Калькулятор;
6. Листы формата А4 (по 1 для каждого члена проекта), для черновых записей
7. Мультимедийное оборудование;
8. Бейджики;
9. Указка.

УСЛОВИЯ ЗАДАЧИ ИГРЫ

Командам необходимо выполнить проектирование компьютерной сети для какой-либо организации. При проектировании необходимо обязательно указать цель (описать назначение проектируемой локальной сети, проектные требования, которым нужно следовать при проектировании локальной сети) проектирования и перечислить задачи, которые необходимо выполнить для достижения поставленной цели.

Проектная документация команды должна содержать план организации с указанием рационального размещения и взаимного расположения локальных абонентских систем, серверов, сетевого оборудования (в соответствии с

планом); техническое задание для приобретения оборудования с указанием их параметров и характеристик). В том случае если помещение организации представляет несколько этажей здания, то необходимо рассмотреть взаимное расположение этажей с указанием на каждом этаже схемы размещения локальных абонентских систем, серверов, сетевого оборудования. Также необходимо охарактеризовать функциональные возможности проекта локальной сети -указать требования к надежности, пропускной способности, масштабируемости, конфигурируемости и перечислить все критерии, которым должна удовлетворять сеть.

Кроме того документация команды содержать требования к топологии и технологии проектируемой локальной сети организации, которая соответствует составленному плану и позволяет обеспечивать информационный обмен в организации с требуемым уровнем надежности и пропускной способности, так же команда должна указать методы доступа к каналам связи и тип среды передачи данных.

Для технико-экономического обоснования проекта локальной сети нужно проанализировать общий состав и стоимость всех компонентов сетевого оборудования, для этого нужно: рассчитать длину всех линий связи по составленному плану расположения локальных абонентских систем, рассчитать стоимость сетевого оборудования и монтажных работ с учетом его количества (примерную стоимость оборудования и монтажных работ найти с помощью Интернет).

В заключительной части работы команда должна сделать выводы по выполненной работе и предполагаемый эффект от проектируемого сетевого обеспечения.

ВАРИАНТЫ ЗАДАНИЯ

Для каждой команды участника определяется своя организация, для которой проектируется компьютерная сеть.

Примерный перечень организаций для проектирования сети представлены в таблице 1

Таблица 1.Перечень организаций для проектирования сети

№	Наименование	Дополнительная информация
1	Проектирование локальной вычислительной сети образовательного учреждения	Количество этажей: 4; Количество компьютеров: 50; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
2	Проектирование локальной вычислительной сети библиотеки	Количество этажей: 2; Количество компьютеров: 30; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
3	Проектирование локальной вычислительной сети социального учреждения	Количество этажей: 3; Количество компьютеров: 40; Количество офисной техники: 30; Площадь помещений и размеры комнат выбираются самостоятельно.
4	Проектирование локальной вычислительной сети муниципального унитарного предприятия	Количество этажей: 2; Количество компьютеров: 40; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
5	Модернизация сетевого взаимодействия администрации МО	Количество этажей: 4; Количество компьютеров: 60; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
6	Проектирование локальной вычислительной сети учреждения культуры	Количество этажей: 2; Количество компьютеров: 30; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
7	Модернизация сетевого взаимодействия торговой фирмы	Количество этажей: 2; Количество компьютеров: 40; Количество офисной техники: 20; Площадь помещений и размеры комнат выбираются самостоятельно.
8	Проектирование локальной вычислительной сети гостиницы	Количество этажей: 5; Количество компьютеров: 40; Количество офисной техники: 10; Площадь помещений и размеры комнат выбираются самостоятельно.
9	Проектирование локальной вычислительной сети многофункционального центра	Количество этажей: 3; Количество компьютеров: 80; Количество офисной техники: 40; Площадь помещений и размеры комнат выбираются

		самостоятельно.

Так же команды имеют право выбрать свою организацию для проектирования.

ПРАВИЛА ПРОВЕДЕНИЯ И ЦЕЛИ ДЕЛОВОЙ ИГРЫ

Преподаватель-организатор представляет членов жюри, объявляет команды и их участников

Продолжительность игры: 4 академических часа (план урока представлен в приложении Б).

Участники разных команд не должны советоваться или делится идеями.

Результатом подготовки команд является проект компьютерной сети для внедрения в какой-либо организации.

Каждая команда должна презентовать свой проект используя средства MS Office Word, Visio, Power Point. Презентация проекта должна включать следующие материалы:

– краткое описание организации, для которой осуществляется проектирование сети;

– описание топологии проектирования,методы доступа к каналам связи и тип среды передачи данных;

– требования к надежности, пропускной способности, масштабируемости, конфигурируемости и критериям, которым должна удовлетворять сеть;

– план организации с указанием мест размещения и расположения локальных абонентских систем, серверов, сетевого оборудования;

– техническое задание на приобретение оборудования для рабочих мест сотрудников организации (серверы, компьютеры и офисная техника);

– сметы на закупку сетевого оборудования и выполнения работ;

– технико-экономическое обоснование проектирования сети;

Участник команды, имеющий роль руководителя проекта, обязан предоставить основные шаги при проектировании, ошибки, допущенные в ходе

проектирования, конфликтные ситуации, возникшие в ходе обсуждения внутри команды и документацию на проектируемую локальную сеть организации.

Инструкционная карта руководителя проекта

Проектную роль можно рассматривать как временную должность в организации (на предприятии).

Руководитель проекта - проектная роль должностного лица, ответственного за управление проектом. Руководитель непосредственно отвечает за достижение целей проекта.

Основные полномочия руководителя проекта в рамках деловой игры:

1. сформулировать цель проектирования;
2. составить план действий, сформировать предложения по достижению цели, осуществлять контроль над их выполнением;
3. сформулировать задачи, которые необходимо выполнить для достижения цели
4. назначить задачи команде проекта (отдельным ее членам) и контролировать их выполнение;
5. требовать от команды проекта выполнение своих ролевых функций;
6. документирование этапов выполнения задач и оформление документации, поступающей от членов команды в электронном документе с помощью MS Office Word;

Инструкционная карта экономиста проекта

«Экономист» - специалист, ответственный за экономическую часть проекта, через него «проходят» все финансовые затраты на реализацию проекта и от правильности его расчетов зависит стоимость реализации. Ошибки, допущенные в расчетах, могут быть критическими для реализации проекта, и конечная стоимость проекта может существенно превышать ожидания. В таком

случае заказчики проектирования могут полностью или частично отказаться от внедрения спроектированной компьютерной сети.

Инструкционная карта «ИТ-специалиста» проекта

«ИТ-специалист» выполняет сопровождение организации по вопросам связанными с информационными технологиями. При реализации проекта выполняет работы, связанные с сопровождением оборудования и офисной техники организации, отвечает за закупку оборудования для организации и составляет техническое задание на закупку оборудования. Кроме этого отвечает за рациональное размещение оборудования и офисной техники организации. Составляет сметы на закупку компьютерной и офисной техники, сетевого оборудования и материалов для реализации компьютерной сети. При выполнении своих обязанностей «ИТ-специалист» может консультироваться с «Техником по компьютерным сетям» и «Монтажником компьютерной сети».

Инструкционная карта «Техника по компьютерным сетям»

«Техник по компьютерным сетям», отвечает за поддержку работоспособности компьютерной сети организации, при проектировании компьютерной сети на него ложится огромная ответственность по выбору топологии и технологий реализации компьютерной сети, методов доступа к каналам связи и типа среды передачи данных компьютерной сети. Кроме того именно он отвечает за развитие компьютерной сети и обеспечение безопасной и бесперебойной компьютерной сети, выполняет сопровождение сетевого оборудования. При проектировании сети отвечает за рациональное размещение сетевого оборудования и офисной техники.

Инструкционная карта «монтажника компьютерной сети»

«Монтажник компьютерной сети», производит расчет стоимости монтажных работ в соответствии с планом размещения оборудования, при реализации проекта производит прокладку и установку кабельных систем и оборудования, а так же настройку оборудования. Кроме того он может осуществлять консультации «Техника по компьютерным сетям» и «ИТ-специалиста» касательно размещения оборудования, для минимизации затрат и облегчения прокладывания линий связи при реализации проекта сети.

Лабораторная работа №1

Установка штекеров RJ45 на кабель UTP5 по стандартам A, B, с подключением телефонной линии, с питанием по витой паре.

1. Цель работы

Научиться обжимать кабель «витая пара» 5-й категории и тестировать полученные соединения.

2. Приборы и материалы:

Кабель «витая пара» 5-й категории, устройство для обжимки кабеля, коннекторы RJ-45.

3. Краткие теоретические сведения

Для построения компьютерных сетей применяются линии связи, использующие различную физическую среду. В качестве физической среды в коммуникациях используются металлы (в основном медь), сверхпрозрачное стекло (кварц) или пластик и эфир. Физическая среда передачи данных может представлять собой кабель "витая пара", коаксиальные кабель, волоконно-оптический кабель и окружающее пространство.

Линии связи, или линии передачи, данных - это промежуточная аппаратура и физическая среда, по которой передаются информационные сигналы (данные).

В одной линии связи можно образовать несколько каналов связи (виртуальных или логических каналов), например, путем частотного или временного разделения каналов. Канал связи - это средство односторонней передачи данных. Если линия связи монопольно используется каналом связи, то в этом случае линию связи называют каналом связи.

Канал передачи данных - это средства двухстороннего обмена данными, которые включают в себя линии связи и аппаратуру передачи (приема) данных. Каналы передачи данных связывают между собой источники информации и приемники информации.

В качестве линий связи могут быть применены коаксиальный кабель или кабель "витая пара".

Витая пара (англ. twisted pair) — вид кабеля связи, представляет собой одну или несколько пар изолированных проводников, скрученных между собой (с небольшим числом витков на единицу длины), покрытых пластиковой оболочкой. Свивание проводников производится с целью повышения связи проводников одной пары

(электромагнитная помеха одинаково влияет на оба провода пары) и последующего уменьшения электромагнитных помех от внешних источников, а также взаимных наводок при передаче дифференциальных сигналов. Для снижения связи отдельных пар кабеля (периодического сближения проводников различных пар) в кабелях UTP категории 5 и выше провода пары свиваются с различным шагом. Витая пара - один из компонентов современных структурированных кабельных систем. Используется в телекоммуникациях и компьютерных сетях в качестве сетевого носителя во многих технологиях, таких как Ethernet, ARCNet и Token ring. В настоящее время благодаря своей дешевизне и лёгкости в установке является самым распространённым решением для построения локальных сетей.

Кабель подключается к сетевым устройствам при помощи соединителя 8P8C (RJ45 или RJ-45), немного большего, чем телефонный соединитель RJ11.

В зависимости от наличия защиты — электрически заземлённой медной оплетки или алюминиевой фольги вокруг скрученных пар - определяют разновидности данной технологии.

Незащищенная витая пара

Неэкранированная витая пара (UTP — Unscreened twisted pair)

— экранирование полностью отсутствует;

Фольгированная витая пара (FTP — Foiled twisted pair) — также известна как S/UTP [1] присутствует один общий внешний экран;

Фольгированная экранированная витая пара (SFTP — Shielded Foiled twisted pair) — отличается от FTP наличием дополнительного внешнего экрана из медной оплетки;

Виды защищенной витой пары:

Стандартная (STP — Shielded twisted pair) присутствет экран для каждой пары;

Экранированная витая пара (S/STP — Screened shielded twisted pair) отличается от STP наличием дополнительного общего внешнего экрана.

Экранирование обеспечивает лучшую защиту от электромагнитных наводок как внешних, так и внутренних, и т. д. Экран по всей длинесоединен с неизолированным дренажным проводом, который объединяет экран в случае разделения на секции при излишнем изгибе или растяжении кабеля. В зависимости от структуры проводников кабель применяется одно- и многожильный. В

первом случае каждый провод состоит из одной медной жилы, а во втором — из нескольких.

Одножильный кабель не предполагает прямых контактов с подключаемой периферией. То есть, как правило, его применяют для прокладки в коробах, стенах и так далее с последующим оконечиванием розетками. Связано это с тем, что медные жилы довольно толстые и при частых изгибах быстро ломаются. Однако для «врезания» в разъемы панелей розеток такие жилы подходят как нельзя лучше.

В свою очередь, многожильный кабель плохо переносит «врезание» в разъёмы панелей розеток (тонкие жилы разрезаются), но замечательно ведет себя при изгибах и скручиваниях. Кроме того, многожильный провод обладает большим затуханием сигнала. Поэтому многожильный кабель используют в основном для изготовления патчкордов (PatchCord), соединяющих периферию с розетками.

Конструкция кабеля

Кабель обычно состоит из четырёх пар. Проводники в парах изготовлены из монолитной медной проволоки толщиной 0,5 - 0,65 мм. Кроме метрической, применяется система AWG, в которой эти величины составляют 24 или 22 соответственно. Толщина изоляции около

0,2 мм, материал обычно поливинилхлорид (английское сокращение PVC), для более качественных образцов 5-й категории - полипропилен (PP), полиэтилен (PE). Особенно высококачественные кабели имеют изоляцию из вспененного (ячеистого) полиэтилена, который обеспечивает низкие диэлектрические потери, или тефлона, обеспечивающего уникалный рабочий диапазонтемператур.

Также внутри кабеля встречается так называемая «разрывная нить» (обычно капрон), которая используется для облегчения разделки внешней оболочки: при вытягивании она делает на оболочке продольный разрез, который открывает доступ к кабельному сердечнику, гарантированно не повреждая изоляциюпроводников.

Внешняя оболочка имеет толщину 0,5 - 0,6 мм и обычно изготавливается из привычного поливинилхлорида с добавлением мела, который повышает хрупкость. Это необходимо для точного облома по месту надреза лезвием отрезного инструмента. Кроме этого начинают применяться так называемые «молодые полимеры», которые не поддерживают горения и не выделяют при нагреве галогенов (такие кабели маркируются как LSZH - Low Smoke Zero Halogen и обычно

имеют яркую окраску внешней оболочки).

Самый распространенный цвет оболочки - серый. Оранжевая окраска, как правило, указывает на негорючий материал оболочки, который позволяет прокладывать линии в закрытых областях. В общем случае цвета не обозначают особых свойств, но их применение позволяет легко отличать коммуникации с разным функциональным назначением как при монтаже, так и обслуживании.

Отдельно нужно отметить маркировку. Кроме данных о производителе и типе кабеля она обязательно включает в себя метровые или футовые метки.

Форма внешней оболочки также может быть различна. Чаще других применяется самая простая - круглая. Только для прокладки под половым покрытием по очевидной причине используется плоский кабель.

Кабели для наружной прокладки обязательно имеют влагостойкую оболочку из полиэтилена, которая наносится (как правило) вторым слоем поверх обычной, поливинилхлоридной. Кроме этого возможны заполнение пустот в кабеле водоотталкивающим гелем и бронирование с помощью гофрированной ленты или стальной проволоки.

Категории кабеля

Существует несколько категорий кабеля „витая пара”, которые нумеруются от CAT1 до CAT7 и определяют эффективный пропускаемый частотный диапазон. Кабель более высокой категории обычно содержит больше пар проводов и каждая пара имеет больше витков на единицу длины. Категории неэкранированной витой пары описываются в стандарте EIA/TIA 568 (Американский стандарт проводки в коммерческих зданиях).

CAT1 (полоса частот 0.1 МГц) - телефонный кабель, всего одна пара (в России применялся кабель без скруток — «лапша», у него характеристики не хуже, но больше влияние помех). В США использовался ранее только в «скрученном» виде. Применяется только для передачи голоса или данных при помощи модема.

CAT2 (полоса частот 1 МГц) - старый тип кабеля, 2 пары проводников, поддерживал передачу данных на скоростях до 4 Мбит/с, использовался в сетях token ring и ARCNet. Сейчас иногда встречается в телефонных сетях.

CAT3 (полоса частот 16 МГц) - 4-парный кабель, использовался при построении локальных сетей 10BASE-T и token ring, поддерживает скорость передачи данных до 10 или 100 Мбит/с по технологии 100BASE-T4. В отличие от предыдущих двух отвечает требованиям

стандарта IEEE
802.3. Также до сих пор встречается в телефонныхсетях.

CAT4 (полоса частот 20 МГц). Кабель состоит из 4 скрученных пар, использовался в сетях token ring, 10BASE-T, 100BASE-T4, скорость передачи данных не превышает 16 Мбит/с по одной паре, сейчас не используется.

CAT5 (полоса частот 100 МГц) - 4- парный кабель, это и есть то, что обычно называют кабель «витая пара» (рис. 8.19). Благодаря высокой скорости передачи до 100 Мбит/с при использовании 2 пар и до 1000 Мбит/с при использовании 4 пар, является самым распространённым сетевым носителем, использующимся в компьютерных сетях до сих пор. При прокладке новых сетей пользуются несколько усовершенствованным кабелем CAT5e (полоса частот 125 МГц), который лучше пропускает высокочастотные сигналы. Ограничение на длину кабеля между устройствами (компьютер-свитч, свитч- компьютер, свитч-свитч) 100 м. Ограничение хаб-хаб 5 м.

CAT6 (полоса частот 250 МГц) применяется в сетях Fast Ethernet и Gigabit Ethernet, состоит из 4 пар проводников и способен передавать данные на скорости до 1000 Мбит/с. Добавлен в стандарт в июне 2002 года. Существует категория CAT6a, в которой увеличена частота пропускаемого сигнала до 500 МГц. По данным IEEE, в 70 % установленных сетей в 2004 году применялся кабель категории CAT6.

CAT7. Спецификация на данный тип кабеля пока не утверждена, скорость передачи данных до 100 Гбит/с, частота пропускаемого сигнала до 600-700 МГц. Кабель этой категории экранирован. Седьмая категория витой пары не UTP, а S/FTP (Screened Fully shielded Twisted Pair). Благода- ря двойному экрану длина кабеля может превышать 100м.

Схемы обжима витой пары

Для обжима витой пары UTP используются разъемы стандарта RJ-45 (рис. 1), которые в зависимости от вида кабеля «витой пары» бывают:

- экранированными илинеэкранированными;

- конструктивно выполненными со вставками или без вставок. Вставки выполняют роль направляющих для проводников «витой пары», упрощающих заправку проводников в корпусразъема;

- для одножильных или многожильных «витыхпар».

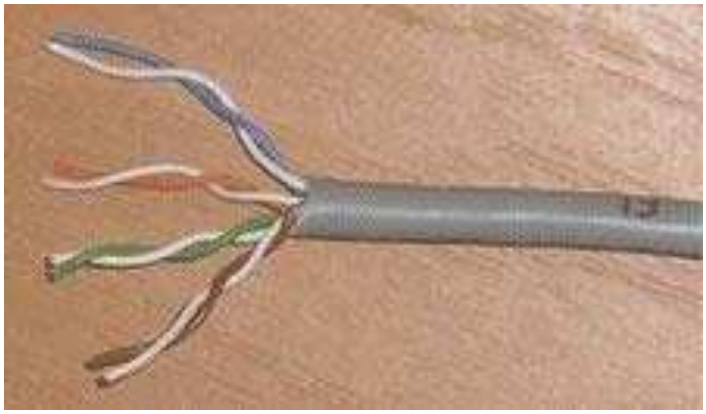


Рис. 1. Кабель из 4 неэкранированных витых пар

Для обжимки «витых пар» используют специальный инструмент, который имеет три рабочие области и соответственно выполняет три функции:

1. Ближе всего к рукояткам устройства располагается область, в которой установлен нож для обрезания проводников «витой пары». Также в этой области есть специальная выемка для снятия внешней изоляции с круглого кабеля (рис.1).

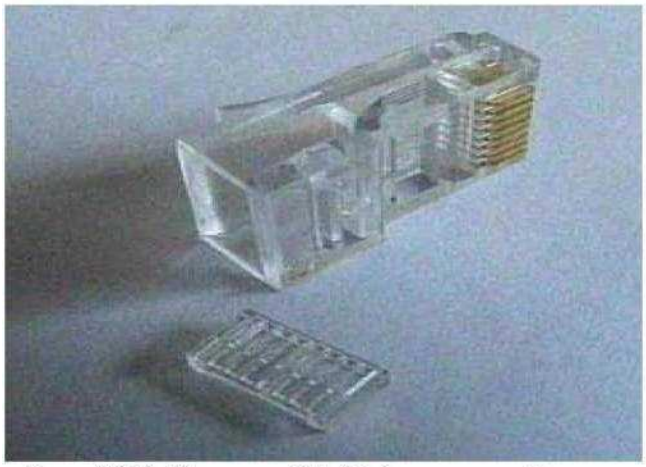


Рис. 8.20. Разъем RJ-45 для «витой пары» + вставка

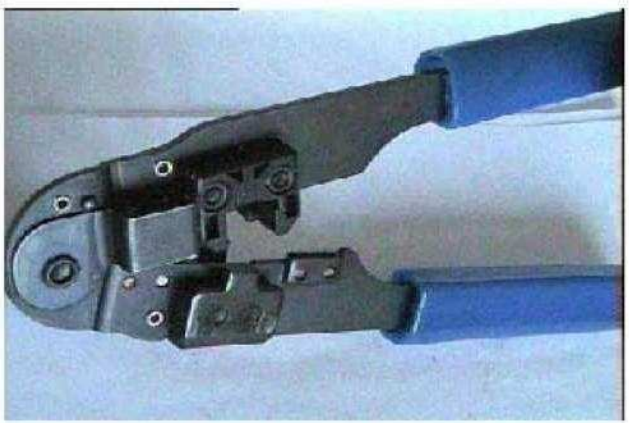


Рис. 2. Устройство для зачистки и обжима сетевого кабеля

2. В центре находится гнездо для обжима разъемаRJ-45.

3. В верхней части устройства, область для зачистки наружной изоляции витой пары UTP (внутренняя изоляция проводников не зачищается, а прорезается контактамиразъема).

Существует две схемы обжимки кабеля: прямой кабель и перекрёстный (Cross-over) кабель (рис. 2).

а)

Рис. 3. Схемы обжимки кабеля: а - прямой кабель

б)

Рис. 4. Схемы обжимки кабеля: б - перекрёстный (кроссовер)

кабель Первая схема используется для соединения

компьютера со свитчем/хабом, вторая для соединения двух

компьютеров напрямую.

4. Ход лабораторной работы

1. Изучить теоретический материал, записав основные моменты лабораторнойработы.
2. Обжать кабель «витая пара» по схемекросс-овер.
3. Вначале проводят зачистку наружной изоляции кабеля. При зачистке плоского кабеля его упирают в специальный выступ на устройстве, расположенный в области зачистки, чтобы получить глубину зачистки под стандартный разъем, зажимают кабель и рывком производят зачистку. Немного более сложным выглядит процесс зачистки круглых кабелей витых пар. Наружную изоляцию круглого кабеля лучше только слегка надрезать, осторожно поворачивая его в области зачистки, а затем снять кусочек изоляции по кольцевому надрезу вручную. На многих обжимных устройствах есть специальная область для снятия внешней изоляции с круглогокабеля.
4. После зачистки разводят провода сетевого кабеля в одной плоскости в необходимом порядке, выравнивают длину всех проводов и еще раз ровно подрезают (рис.6).

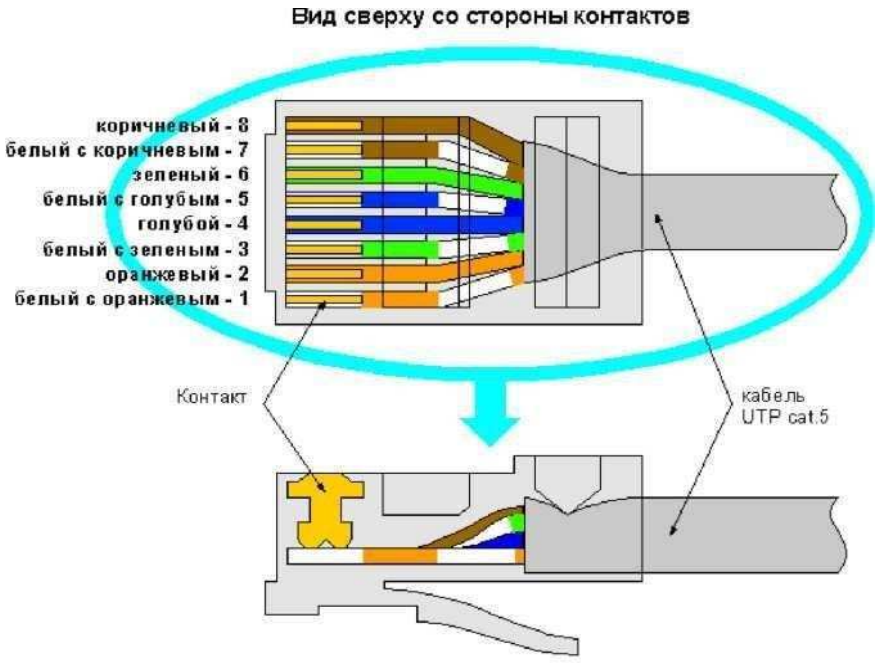


Рис. 6. Схема разводки кабеля

Затем производят заправку проводников в разъем и опрессовку. Рекомендуется по возможности, использовать разъемы без вставки, так как процесс заправки проводников в корпус такого разъема выполняется проще:

а) Если конструктивно разъем выполнен без вставки, то проводники аккуратно заправляются в его корпус до упора в торец

разъема. Затем вставляют разъем в гнездо обжимного устройства и надавливают до тех пор, пока устройство полностью незакроется.

б) Если в конструкцию разъема входит вставка, то сначала на проводники «витой пары» надевается вставка. Вставка имеет форму крышки спичечного коробка, на одной из поверхностей которого имеются прорези по количеству проводников в витой паре. Вставку надевают на проводники таким образом, чтобы прорези были обращены к корпусу разъема. После насаживания вставки проводники витой пары еще раз подрезают и выравнивают срез с краем вставки. Для закрепления вставки в этом положении полезно у ее противоположного конца обжать витую пару пальцами, чтобы вставка не смещалась. Затем вставку с проводниками вставляют в корпус разъема до тех пор, пока она не упрется в торец разъема, и обжимают разъем также, как в случае разъема без вставки.

Контрольныевопросы

1. Строение кабеля «витая пара».
2. Чем отличаются кабели «витая пара» различныхкатегорий?
3. Каковы ограничения на применение «витойпары»?
4. Чем различаются схемы соединения „прямой кабель” и „перекрёстныйкабель”?

Лабораторная работа №2

Настройка сетевых интерфейсов в ОС Windows

Задание:

1. Настроить сетевой интерфейс используя оснастку “Сетевые подключения” (ncpa.cpl). Задать IP адрес, маску, шлюз статически. Настроить сетевой интерфейс таким образом чтобы ваш компьютер входил в одну сеть с компьютером соседа.Проверить достижимость соседа командой ping.
2. Настроить сетевой интерфейс используя оснастку “Сетевые подключения” (ncpa.cpl) так чтобы он получал настройки автоматически с сервера DHCP.
3. Изучить возможности команды ipconfig.
4. Изучить возможности команды arp.

Содержание отчета:

1. Цель работы.
2. Описание проделанной работы по каждому пункту.
3. Выводы по проделанной работе.

Лабораторная работа №3

Настройка сетевых интерфейсов в ОС Linux

Прежде, чем начать выполнение лабораторной работы

1. Изучите материал о адресации узлов в компютерных сетях. Убедитесь, что Вы понимаете, что такое:

- IP адрес, маска сети, в чем отличие IPv4 от IPv6;
- MAC адрес;
- протоколы ARP и ICMP.

2. Прочитайте электронную документацию по следующим утилитам:

- ip
- ifconfig
- ping
- arp

Задание на лабораторную работу

1. Используя утилиту ip, определите, сколько сетевых подключений имеется в системе?
2. С помощью утилиты ifconfig попытайтесь найти, сколько сетевых подключений уже сконфигурировано и активно?
3. Заданы ли адреса для каждого сетевого подключения?
4. Задайте адрес с помощью утилилиты ip - 192.168.1.2, маска - 255.255.255.0. Команда: ip addr add IP_адрес/маска dev имя_интерфейса
5. Используя команду ip научится включать, выключать интерфейс: ip link set имя_интерфейса up\down. Проверить командой: ip link show.
6. Используя команду ip - удалить настройки IP адреса сетевого интерфейса.
7. Задайте адрес 10.0.0.1 с маской 255.0.0.0 для интерфейса eth0 используя утилиту ifconfig.
8. Используя ifconfig научитесь включать/выключать интерфейс.
9. Задайте другой ip адрес из этой сети 10.0.0.0/8, такой - чтобы не было совпадений с другими хостами.
10. Проверьте "наличие связи" (с использованием утилиты ping) до всех других компьютеров. Составьте таблицу с результатами тестирования. В
11. Определите MAC адреса (с использованием утилиты arp) для всех узлов в этой сети.
12. Настройте сетевой интерфейс редактируя файл /etc/network/interfaces. Добавьте настройки для интерфейса eth0: address 192.168.0.2; netmask 255.255.255.0; gateway: 192.168.0.1
13. Включите dhcp клиент для автоматического получения настроек на интерфейсе.

14. Пропишите в файл /etc/network/interfaces настройки для запуска dhcp клиента при старте системы.
15. Добавьте alias-интерфейс eth0:1 с следующими настройками: address: 192.168.1.2, netmask: 255.255.255.0, gateway: 192.168.1.1
16. Проверить доступность alias-интерфейсов соседей.

Содержание отчета:

1. Цель работы.
2. Описание проделанной работы по каждому пункту.
3. Выводы по проделанной работе.

Лабораторная работа №4

Установка, настройка коммутатора Cisco

Цель работы: Ознакомиться с основными командами настройки, контроля и устранения неполадок коммутаторов Cisco.

Задание:

1. Подключиться к коммутатору
2. Изучить характеристики коммутатора выполнив команды и проанализировав их вывод: “?”, show clock, show version, show run (предварительно перейдите в контекст администратора: enable), show arp, show vlan, show interfaces, show interfaces vlan 1, show ip interface brief, show line,
3. Изменить IP адрес виртуального интерфейса коммутатора. Для этого перейти в контекст глобального конфигурирования, затем в контекст конфигурирования 1-го vlan’a.

```
sw> enable
sw# conf t
    sw(config)# interface vlan 1
    sw(config)# ip address 192.168.0.1 255.255.255.0
    sw(config)# no shutdown
```

Подсоеденить компьютер к первому порту коммутатора.

Протестировать достижимость коммутатора выполнив ping 192.168.0.1

4. Изучить web интерфейс управления коммутатором.

Содержание отчета

1. Цель работы.
2. Описание проделанной работы по каждому пункту.
3. Основные параметры коммутатора, настроенные в процессе работы.
4. Выводы по проделанной работе.

Лабораторная работа №5

Установка, настройка маршутизатора Cisco

Задание:

1. Идентифицировать порты
2. Идентифицировать световые индикаторы
3. Подключить маршрутизатор силовым кабелем к сети. Подключить компьютер кабелем-витая пара к маршрутизатору (правильно выбрать тип кабеля!). Подключиться к консольному порту маршрутизатора.
4. Изучить характеристики маршрутизатора, выполнив команды и изучив их вывод: show processes; show clock; show interfaces; show running-config; show mac-address-table; show ip interface brief; show users (Возможно некоторых команд нет в текущей версии ОС маршрутизатора).
5. Настроить сетевой интерфейс компьютера и маршрутизатора так чтобы они были в одной сети.
6. Проверить с маршрутизатора достижимость компьютера и наооборот.
7. Настроить имя маршрутизатора (команда hostname)

Содержание отчета

1. Цель работы.

2. Описание проделанной работы по каждому пункту.

3. Выводы по проделанной работе.

Лабораторная работа №6

Разбиение сети на подсети

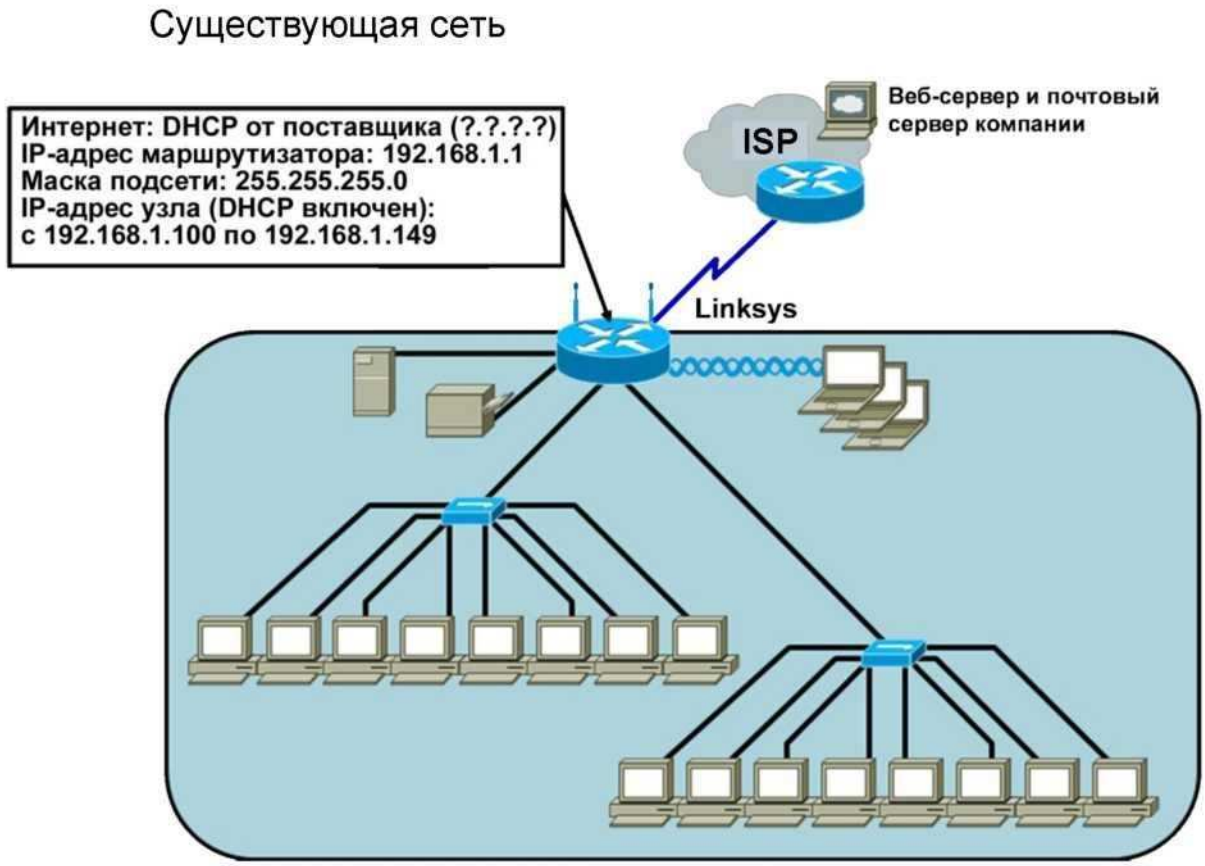
Цель: Создать план IP-адресации для небольшой сети

Задание:

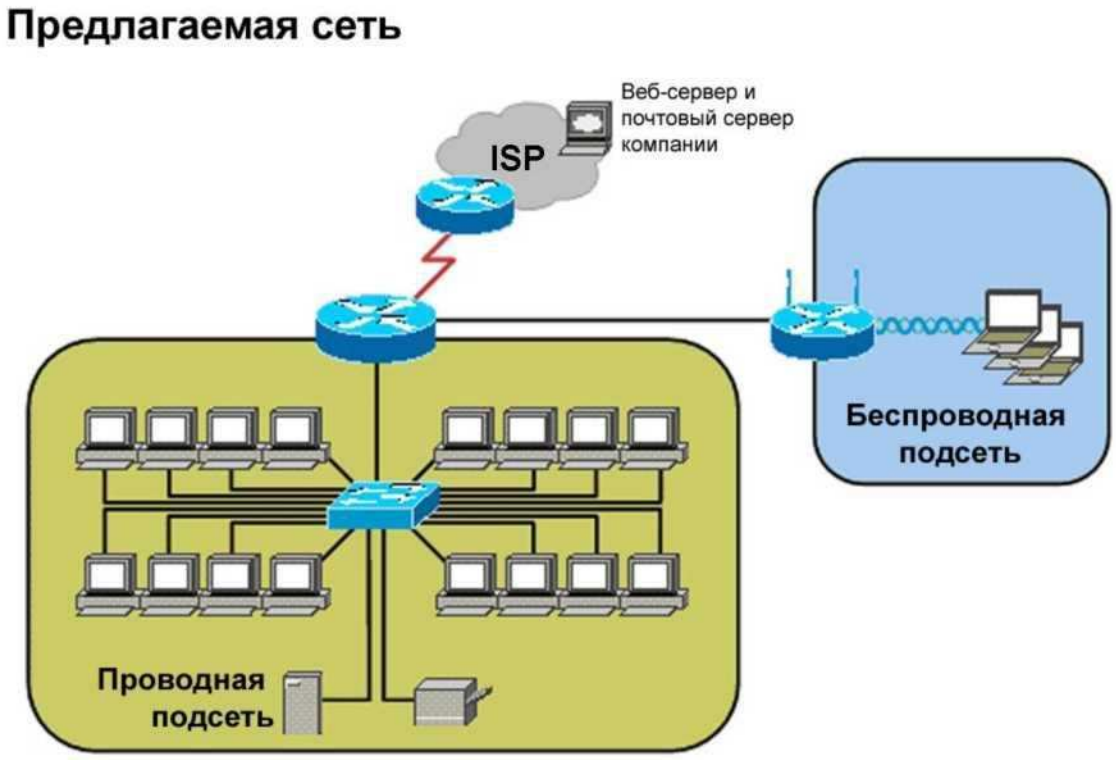
Основная информация и сведения для подготовки

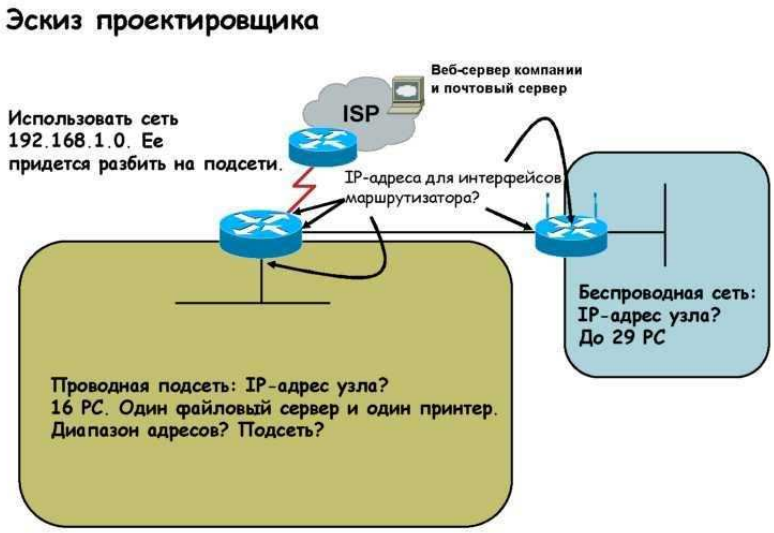
В этой лабораторной работе необходимо выполнить функции сотрудника поставщика услуг Интернета (ISP), заключающиеся в оказании услуг по установке и поддержке у клиентов.

Клиент позвонил ISP, жалуясь на проблемы с электронной почтой и перебои в работе Интернета. На предыдущем вызове техник создал схему существующей сети клиента.



ISP готовит проекту совершенствования сети. Предварительная топологическая схема представлена ниже.





Один из сетевых проектировщиков ISP сделал некоторые заметки на эскизе проектируемой сети и указал некоторые требования. Проектировщик просит нас разработать план IP-адресации для данной сети.

Шаг 1. Анализ сети

а. Согласно эскизу проектировщика определите минимальное количество узлов, необходимое подсети для обеспечения нормальной работы проектируемой сети.

1) Самая большая подсеть должна поддерживать узлов.
2) Для поддержки такого количества узлов необходимо отведенных

для них бит.

б. Какое минимальное количество подсетей необходимо для новой сети?

в. Может ли эта сеть быть разделена на подсети согласно требованиям?

Пример. Еслинеобходимычетыреподсети, самаябольшаяизкоторыхдолжнаподдерживать 128 узлов, томыстолкнемсяспроблемой, потомучтоподсетьсетиклассаС, разбитаяна 4 подсети, можетподдерживатьтолько 62 узла.

г. Заполнитепустыеместа, чтобысуммироватьтребованиякподсетямдляпроектируемойсети:

Дляэтойсетитребуется подсети, каждаяизкоторыхподдерживает 29 узлов.

Следовательно, дляидентификацииподсетизаняты бита, определяющиеузел.

Притакихзначенияхэтасетьподдерживаетподсетей, каждаяизкоторыхсодержитузлов.

Шаг 2. Расчетпользовательскоймаскиподсети

Когдачислобитов, отведенныхнаIDподсети, известно, можновычислитьмаскуподсети. ВсетиклассаСмаскаподсетипоумолчаниюсодержит 24 бита, или 255.255.255.0. Какойбудетпользовательскаямаскаподсети?

Пользовательскаямаскаподсетидляданнойсетибудет . . . , или / .

Шаг 3. Определение IP-адресов узлов

Поскольку маска подсети определена, можно создать схему адресации сети. Схема адресации состоит из номеров подсетей, широковещательного адреса подсети и диапазона IP-адресов, назначаемых узлам.

а. Заполните таблицу, в которой представлены все возможные подсети для сети 192.168.1.0.

Подсеть	**Адрес подсети**	**Диапазон IP-адресов узлов**	**Широковещательный**

б. Следующая таблица прилагалась к схеме с заметками проектировщика вместе с просьбой о ее заполнении. Узлам будут присвоены IP-адреса следующим образом (заполните приведенную ниже таблицу):

Устройств	**Интерфей**	**IP-адрес**	**Подключение к**	**IP-адрес**
1841	Serial 0/0/0	11.11.11.100	Маршрутизатор ISP	11.11.11.1
	Fa 0/0		Проводные узлы	Диапазон проводного узла: от
				До
	Fa 0/1		Интернет Linksys	
Linksys	Интернет		1841 Fa 0/1	
	Шлюз локальной сети		Беспроводные узлы	Диапазон беспроводного узла: от
				До

Шаг 4. Рассмотрение альтернативных вариантов организации подсети

А что, если бы было более 30 узлов, которые должны поддерживаться проводной либо беспроводной частью сети. Можно использовать меньше битов и создать меньше подсетей, при том, что каждая будет поддерживать большее число узлов в расчете на подсеть.

а. Сколько потребуется битов, чтобы создать четыре подсети?

б. Сколько битов останется для узлов в каждой подсети?

в. Какое максимальное количество узлов сможет поддерживать каждая подсеть?

г. Какой будет маска подсети в точечно-десятичном формате и в формате косая черта-номер (/#)?

д. Если начать с той же сети 192.168.1.0, как и ранее, и разбить ее на четыре подсети, какие IP адреса будут у подсетей?

Шаг 5. Создание тестового стенда разработанной сети.

Постройте указанную топологию в программе CiscoPacketTracer. Добавьте необходимое количество оборудования. Настройте IP адресацию на каждом узле сети. (Внимание ping не будет работать из беспроводной сети в проводную – т.к. не настроена маршрутизация).

Лабораторная работа №7

Управление учетными записями и правами доступа в Microsoft Windows

Цель работы: ознакомление со способами управления учетными записями и правами доступа в операционных системах семейства MicrosoftWindows

Компьютерная программа :VirtualBox с установленной операционной системой WindowsServer 2008

Порядок выполнения работы:

1. Запустить виртуальную машину с установленной ОС WindowsServer 2008 R2.
2. Открыть оснастку для управления локальными пользователями и группами. Поменять пароль для учетной записи **Administrator**на: **123qweRTY**
3. Настроить рабочую группу для компьютера: **524**, имя ПК: **524-ваша-фамилия** (вместо ваша_фамилия – надо написать СВОЮ фамилию на английском языке, например**524-ivanov, 524-petrov**).
4. Создать локального пользователя: login – **ваша-фамилия**, password – **passWORD123**.Сделать это вручную (с помощью оснастки для управления локальными пользователями), затем удалить вручную. Сделать это с помощью утилиты командной строке, затем удалить пользователя с помощью утилиты командной строки. Добавить пользователя снова любым способом.
5. Создать пользовательскую группу **vt** и включить в нее пользователя **ваша-фамилия**. Сделать это вручную (с помощью оснастки), затем удалить вручную. Сделать это с помощью утилиты командной строки, затем удалить с помощью утилиты командной строки.
6. Разрешить удаленный доступ к Виртуальной машине. Добавить созданного в шаге (4) пользователя **ваша-фамилия** в группу **RemoteUsers**.
7. Подключиться к соседнему серверу, с помощью программы **Подключение к удаленному рабочему столу** (проверьте корректность настроек сетевого подключения, и настроек **Сети** в программе **VirtualBox**).
8. Когда сосед подключится к вашему серверу, найдите его в диспетчере задач. Выпишите **имя пользователя**, **тип сеанса** и **имя клиента**.
9. Вывести всех пользователей системы с помощью утилиты командной строки (команлаqwinsta).
10. Создатьпапки**C:\onlyread**, **C:\all, C:\closed**. Назначить пользователю **ваша-фамилия** для папок следующие разрешения: для папки **all** установить **Полный доступ;** для папки **onlyread** установить чтение и выполнение, запретить запись; для папки **closed** запретить все. Выполнить вход под учетной записью **ваша-фамилия** и проанализировать доступность папок для чтения записи, создания новых файлов, папок. Ответить на вопросы в таблице.

Папка / Вопрос	all	onlyread	closed
Можно ли прочитать содержимое папки – открыть папку			
Можно ли создать подпапку			
Можно ли создать файл			
Можно ли удалить папку			

11. Оформить типовой отчет (содержащий титульный лист и второй лист с указанием номера работы и кода специальности) со скриншотами, для каждого ключевого пункта работы.

Контрольные вопросы

1. Что такое учетная запись пользователя?
2. Что такое разрешения?
3. Что такое права?
4. В каких случаях удобнее создавать пользователей с помощью утилит командной строки?
5. Как называется оснастка для управления локальными пользователями?
6. Для чего используется группа RemoteUsers?
7. Какие учетные записи вы используете при аутентификации на удаленном компьютере?
8. В каком диалоговом окне вы настраивали удаленный доступ к компьютеру?
9. Какие типы объектов доступа вы знаете?
10. Как можно посмотреть локальных пользователей в ОС Windows?
11. Где в операционной системе можно посмотреть активных пользователей?
12. В чем различие между интерактивным и локальным пользователем?

Лабораторная работа №8
Управление сетевыми службами в Microsoft Windows

Цель работы: ознакомление со способами управления сетевыми службами в операционных системах семейства Microsoft Windows

Компьютерная программа: программный продукт виртуализации VirtualBox с установленной операционной системой Windows Server 2008

Порядок выполнения

Часть 1. DNS-сервер

1. Подключиться к серверу **virtual**. Открыть программу **VirtualBox**. Запустить виртуальную машину с установленной операционной системой WindowsServer 2008 R2.
2. Открыть **Диспетчер Сервера.**
3. Добавить роль **DNS сервер**, установить роль с помощью **Мастера добавления ролей.**
4. Открыть оснастку **Службы.** Найти службу **DNS-сервер**. Выписать в отчет следующие поля: **описание; состояние; тип запуска; вход от имени.** Открыть **Свойства** вкладку **Восстановление** и выписать действие компьютера, выполняемое при сбое службы.
5. Открыть **Брандмауэр.** Найти **правила для входящих подключений** касающиеся работы службы **DNS-сервер.** Найти **правила для исходящих подключений** касающиеся работы службы **DNS-сервер**. Выписать все правила. Для каждого правила открыть диалоговое окно **Свойства** и выписать **имя правила, описание правила**, **тип протокола, номер протокола, локальный порт, удаленный порт.**
6. Открыть консоль управления DNS-сервером. Открыть диалоговое окно **Свойства**DNS-сервера. Перейти на вкладку **Сервер Пересылки.** Добавить сюда известный вам DNS-сервер (сервер учебного заведения).
7. Создать новую зону прямого просмотра. Тип зоны: **основная зона**, имя зоны: **ваша-фамилия.local**, создать новый файл, запретить динамические обновления.
8. Запустить утилиту nslookup. Разрешить имя **имя-вашего-компьютера.имя-вашего-домена.local**(имя должно выглядеть следующим образом: **524-ваша-фамилия.ваша-фамилия.local**). Сделайть так, чтобы DNS-сервер, разрешал имя вашего сервера в IP-адрес.
9. Добавить в зону прямого просмотра записи (A) про: file-server, app-server, print-server. IP адреса выбрать самостоятельно, так чтобы сервера находились в одной подсети с DNS-сервером.
10. Запустить nslookup. Проверить, что DNS-сервер умеет разрешать доменные имена: **file-server.ваша-фамилия.local, app-server.ваша-фамилия.local, print-server.ваша-фамилия.local.**
11. Разрешить IP-адреса, соответствующие DNS-серверу, file-server, app-server, print-server в доменные имена. В отчете написать вывод о полученных результатах.
12. Создать **зону обратного просмотра.** Тип зоны: **основная зона;зона обратного просмотра IPv4.**
13. Добавить в обратную зону, записи про: DNS-сервер, file-server, app-server, print-server.

14. Запустить nslookup. Проверить, что DNS-сервер разрешает IP-адреса: DNS-сервера, file-server, app-server, print-server.
15. Создатьпсевдонимы (CNAME), **apps**для**app-server**, **files**для**file-server**, **print** для **print-server**.
16. Запустить**nslookup**. Разрешитьимена apps.ваша-фамилия.local, files.ваша-фамилия.local, print.ваша-фамилия.local.
17. В существующей зоне прямого просмотра создать новый домен **hr.ваша-фамилия.local**. Внутри этого домена, создать запись типа (A) для компьютера **pc1,**IP-адрес выбрать самостоятельно.
18. Запустить nslookup. Убедиться, что DNS-сервер разрешает имя **pc1.hr.ваша-фамилия.local.**
19. Приостановить DNS-сервер. Открыть nslookup, разрешить имена: apps.ваша-фамилия.local, files.ваша-фамилия.local, print.ваша-фамилия.local. В отчете сделать вывод, о результатах работы утилиты nslookup.
20. Запустить DNS-сервер.

Часть 2. DHCP-сервер

1. Открыть Диспетчер сервера.
2. Добавить роль **DHCP-сервер**. Настройки при установке задать следующие: **Выбор привязки сетевого подключения** выбрать настроенный статически IP-адрес; **Указать параметры IPv4 DNS-сервера –** указать родительский домен (ваша-фамилия.local), проверить адрес основного сервера; **Задать параметры IPv4 WINS-сервера** – WINS не требуется для приложений в этой сети; создать новую область с именем **ваша-фамилияScope;** для новой области задать начальный и конечный IP-адрес, основной шлюз, dns-сервер; **Настроить режим DHCPv6 без отслеживания состояния –** Отключить режим без отслеживания состояния DHCPv6 для этого сервера.
3. Открыть оснастку **Службы.** Найти службу **DHCP-сервер**. Выписать в отчет следующие поля: **описание; состояние; тип запуска; вход от имени.** Открыть **Свойства** вкладку **Восстановление** и выписать действие компьютера, выполняемое при сбое службы.
4. Открыть **Брандмауэр.** Найти **правила для входящих подключений** касающиеся работы службы **DHCP-сервер.** Найти **правила для исходящих подключений** касающиеся работы службы **DHCP -сервер**. Выписать все правила. Для каждого правила открыть диалоговое окно **Свойства** и выписать **имя правила, описание правила**, **тип протокола, номер протокола, локальный порт, удаленный порт**
5. Открыть консоль управления DHCP-сервером. Изучить содержимое консоли. (стр 621)

Контрольные вопросы

1. Что такое сетевые службы?
2. Как расшифровывается DNS?

3. Какие функции выполняет DNS-клиент?
4. Какие функции выполняет DNS-сервер?
5. Для чего используется утилита nslookup?
6. Можно ли организовать работу службы DNS автономно (без связи с сетью Интернет) ?
7. Для чего нужна зона прямого просмотра?
8. Для чего нужна обратная зона DNS?
9. Как работает рекурсивная схема разрешения имен?
10. Как работает не рекурсивная схема разрешения имен?
11. Как расшифровывается DHCP?
12. Режимы работы DHCP сервера?
13. Что такое DHCP-агент, зачем он применяется?
14. Алгоритм работы DHCP?
15. Что такое области адресов (scope)?
16. Что такое «исключения» в DHCP?

Лабораторная работа №9

Установка и настройка HTTP-клиента и HTTP-сервера, FTP-клиента и FTP-сервера

Цель работы: Научиться устанавливать и настраивать HTTP-клиент/сервер, FTP-клиент/сервер

Компьютерная программа : программа виртуализации VirtualBox с установленной операционной системой WindowsServer 2008

Порядок выполнения

Часть 1. Выполнить в виртуальной машине для WindowsServer 2008.

Установить роль Web-Server (IIS). Установитьслужбы FTP, FTP Management Console. Настроитьразрешениедоступак web, ftp серверамчерезбрандмауэр, вкладка "Исключения" флажки "FTP Server", "World Wide Web Services (HTTP)".

Для web-сервера добавить виртуальный каталог C:\mysite, псевдоним: mypage.

Запустить сервис FTP-сервера. Установить для службы FTP Publishing Service режим автоматического запуска.
Задать права доступа к FTP-узлу. Запретить анонимные подключения.

Проверить работу web, ftp - серверов http://localhost, ftp://localhost.
Просмотреть текущих пользователей ftp сервера: current sessions - параметры текущих подключений.

Часть 2. Выполнить в виртуальной машине для ОС Ubuntu.

1) Установить HTTP-сервер Apache:

sudo apt-get install apache2

2) Проверить работоспособность сервера Apache, набрать в браузере IP-адрес машины, или 127.0.0.1

3) Файлы хоста находятся в директории /var/www/

Изменить файл index.htmlдобавив в тело документа свою фамилию (например I.Ivanov). Проверить выводится ли фамилия в браузере.

4) Открыть в браузере сервер соседа.
5) Изучить утилиту apache2ctl:

apache2ctlstop – остановить сервер
apache2ctlstart – запустить сервер
apache2ctl restart – перезапустить сервер

6) Выключитьавтозапуск Apache: sudo update-rc.d -f apache2 remove
7) Проверить работу HTTP-сервера выполнив запрос:

-Открыть gnome-terminal → (Поиск на компьютере и в интернете) →Ввести в поле gnome-terminal. Выполнить:
TelenetIPадрес 80
GET /index.htmlHTTP/1.1

Host: IPадрес
(перевод строки)
(перевод строки)
- Прочитать и разобрать ответ HTTP-сервера.

8) Установить сервер FTP.

sudo apt-get install vsftpd

vsftpd – этосервисFTP,доступныйвUbuntu. В процессе установки создается пользователь ftp с домашним каталогом /srv/ftp. Это каталог по умолчанию для FTP.

9) Открыть в браузере ftp://127.0.0.1

Контрольные вопросы

1. Расскажите про HTTP протокол?
2. Расскажите про заголовки в HTTP?
3. Как выглядит строка ответа сервера?
4. Расскажите про протокол FTP?

Лабораторная работа №10
Настройка и использование средств удаленного администрирования и удаленного доступа

Цель работы: ознакомление со способами настройки и использования средств удаленного администрирования и удаленного доступа: telnet, ssh, удаленный рабочий стол, удаленный помощник, vnc, teamviewer.
Компьютерная программа: VirtualBox с установленной операционной системой WindowsServer 2008; компьютер или виртуальная машина с ОС семейства Unix

Постановка задачи или ситуации

В этой работе Вам необходимо установить и настроить средства удаленного доступа. Работа состоит из двух частей, для операционных систем двух семейств – Windows, Unix.

Про Telnet

Есть несколько причин для того, чтобы настраивать сервер Windows 2008 в качестветelnet-сервера. Вот их список:

- Выполнение удаленных команд из командной строки на сервере Windows 2008 через WAN или LAN.
- Возможность настраивать и решать проблемы с различными удаленными устройствами: маршрутизаторами Cisco, серверами Linux, серверами Windows 2008 через интерфейс командной строки.
- Для проверки сервера и с сервера, используя простой и надежный протокол.

Поговорим о примере. Предположим, вы хотите проверить состояние некоторых файлов, которые предполагается передавать на сервер IIS . Есть несколько простых команд, годных для данной цели, и если у вас есть доступ к командной строке Windows, вы можете выполнить их очень быстро. Например, вместо соединения с сервером через RemoteDesktop (RDP), либо VNC, либо еще какой-нибудь метод удаленного контроля, почему бы не выполнить всего 2 команды, получив доступ к серверу через telnet?

Про удаленного помощника

Если Вам надо администрировать рабочие станции пользователей в Вашей сети, к примеру, подключиться к пользователю, посмотретьчто у него не, получается, посмотреть последовательность действий приводящих к ошибке да многое чего. Для этих целей существует много разного стороннего софта, но лучше пользоваться тем, что предоставляет сама операционная система Windows. Это удалённый помощник.

Управление Удаленным помощником может потребовать выполнения настроек для порта 3389, объектов Групповой политики и выполнения ряда других административных задач.

Для управления Удаленным помощником администраторам доступны следующие технологии:

- Брандмауэр. Открывая или перекрывая брандмауэром соединения через порт 3389, администраторы могут определять, может ли служащий Вашей организации запрашивать помощь за ее пределами.
- Групповая политика. С помощью Групповой политики Вы можете разрешать или запрещать запросы помощи с использованием Удаленного помощника. Также Вы можете определить, смогут ли пользователи разрешать эксперту контролировать их компьютер, или только наблюдать за ним. Кроме того, Вы можете настроить Групповую политику, чтобы разрешить или запретить эксперту предлагать удаленную помощь без предварительного запроса от пользователя.
- Отдельный компьютер. Администратор отдельно взятого компьютера может выключить на нем возможность отправки приглашений удаленного помощника, что предотвратит его использование кем бы то ни было.

Порядок выполнения

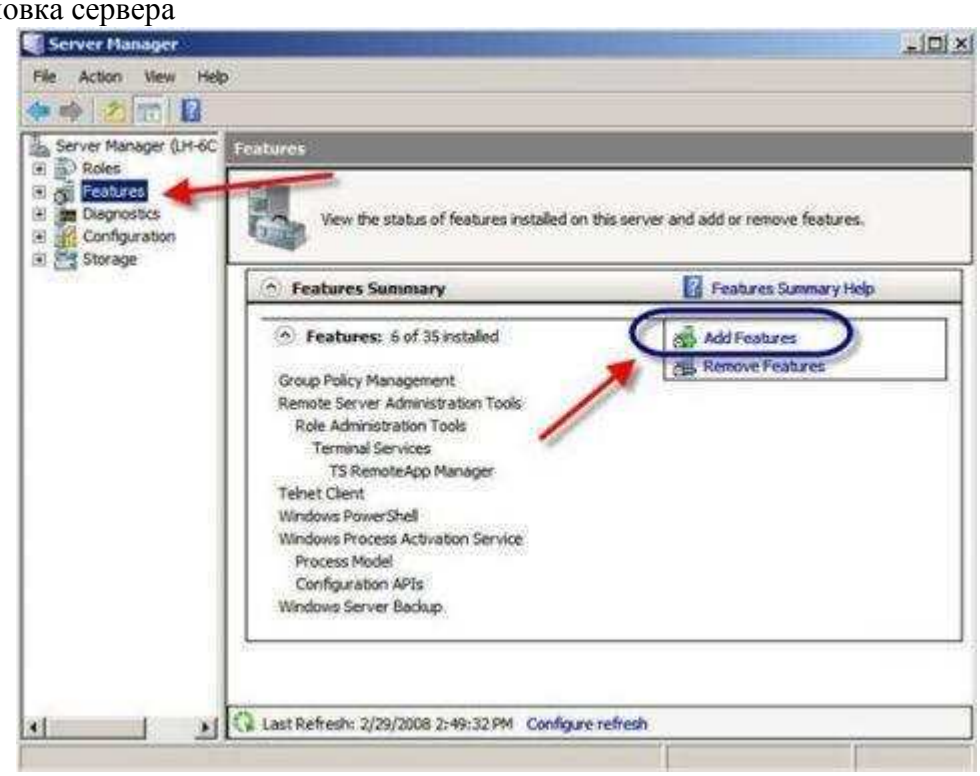
Часть 1. Выполнить в ОС Windows

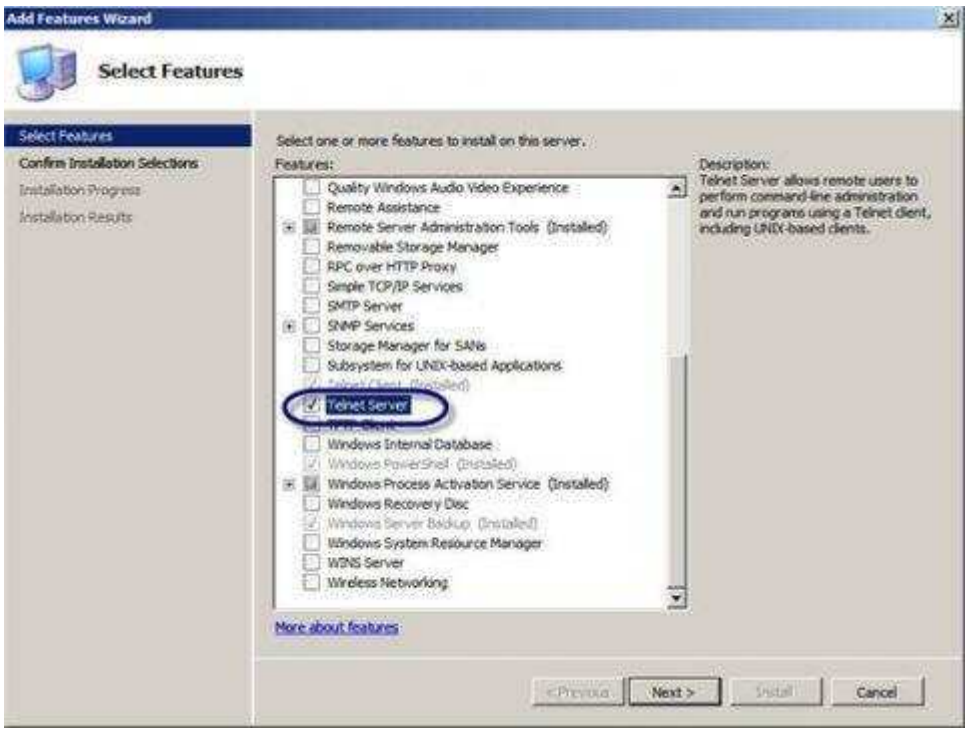
12. Настроить сервер Telnet

a. Установить Telnet сервер, Telnet клиент.
b. Запустить службу Telnet сервера в оснастке **Службы (Services)**. Поменять для службы режим запуска на **автоматический**.
c. С помощью утилиты netstat убедиться, что Telnet сервер работает и слушает 23 порт
d. С помощью утилиты командной строки остановить и запустить сервер, проверить что после остановки сервер больше не «слушает» 23 порт.
   netstoptelnet
   netstarttelnet
e. На данный момент при попытке подключения к серверу вам предложат ввести входные данные. Вы можете получить доступ в качестве администратора, а все остальные пользователи – не администраторы получить доступ не могут. Чтобы дать возможность другим пользователям удаленно подключаться через telnet, нужно изменить специальные настройки. Для этого нужно добавить нужного пользователя в локальную группу **TelnetClients**.Добавить локального пользователя отличного от администратора в эту группу.
f. Подключиться к telnet-серверу соседа: telnetip_адрес_соседа
   Выполнить вход. Ввести логин и пароль локальной учетной записи товарища т.к. вы хотитеудаленно управлять его сервером.Вывести список каталогов диска C:\ (команда dir).
g. Когда сосед будет подключен к вашему серверу выведите список пользователей Telnet сервера:
   tlntadmn –s
h. Отправить сообщение подключенному к вашему серверу соседу:
   tlntadmn –mall “текст сообщения”

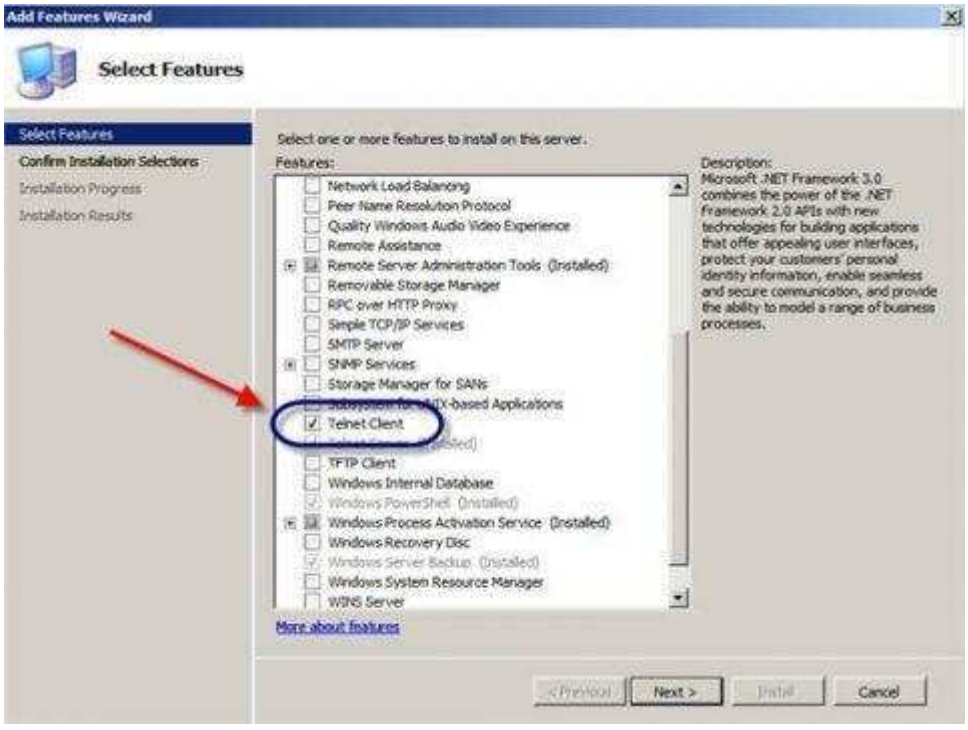
   Ниже приводятся картинки с некоторыми основными шагами:

Установка сервера



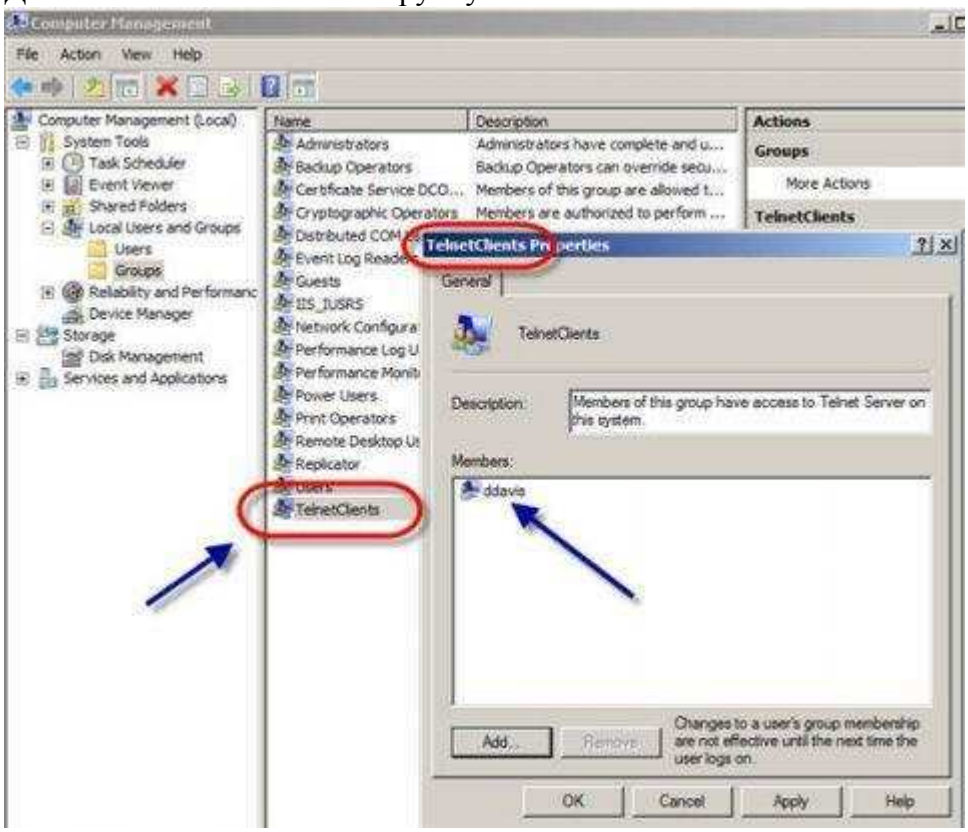


Установка клиента

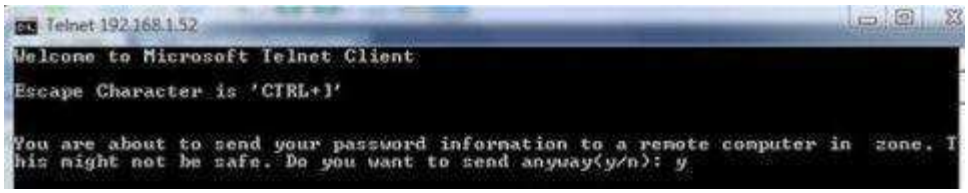


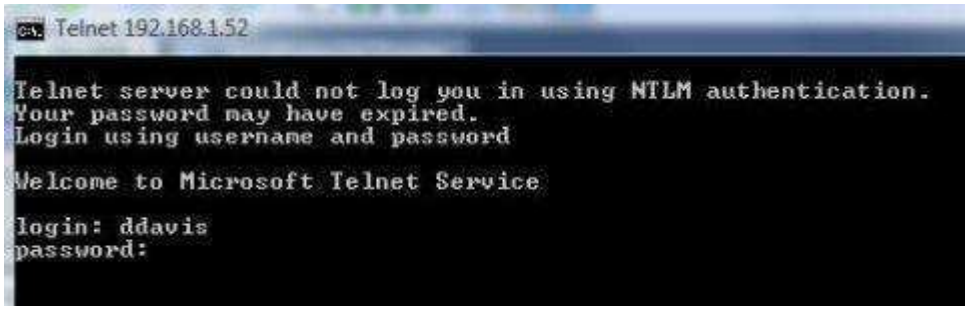
Настройка службы

Добавление пользователя в группу

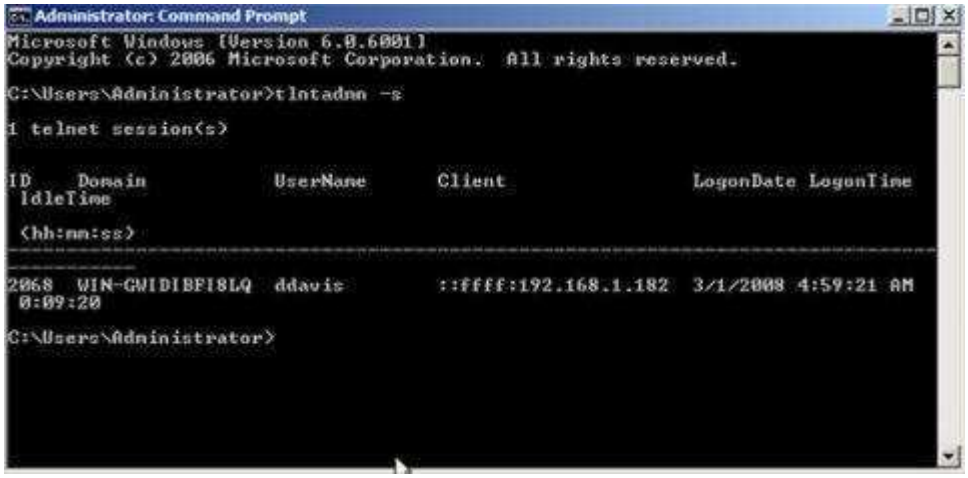


Подключение к серверу



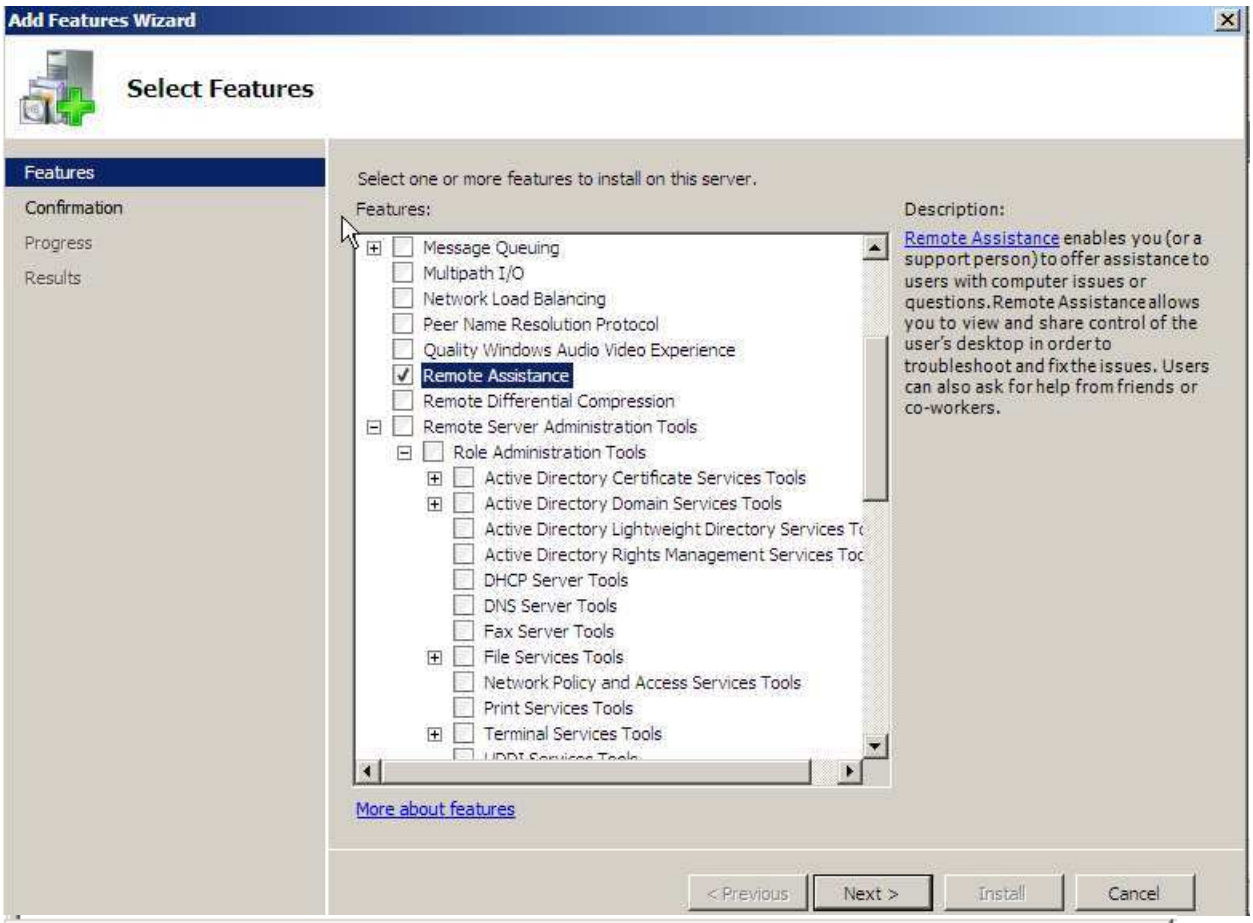


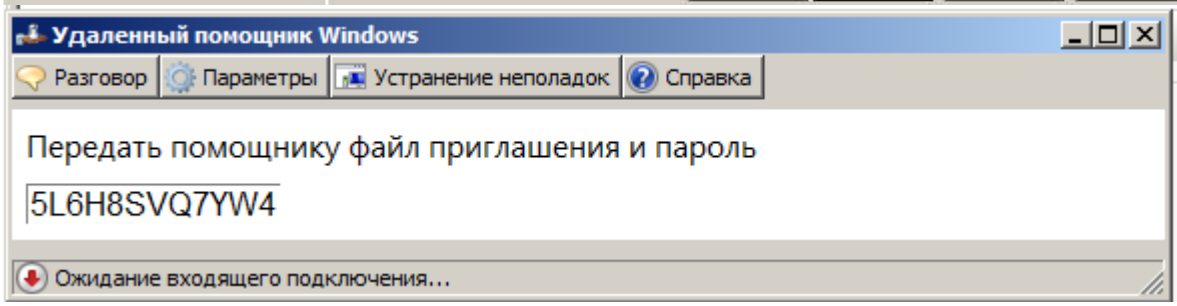
Вывод пользователей

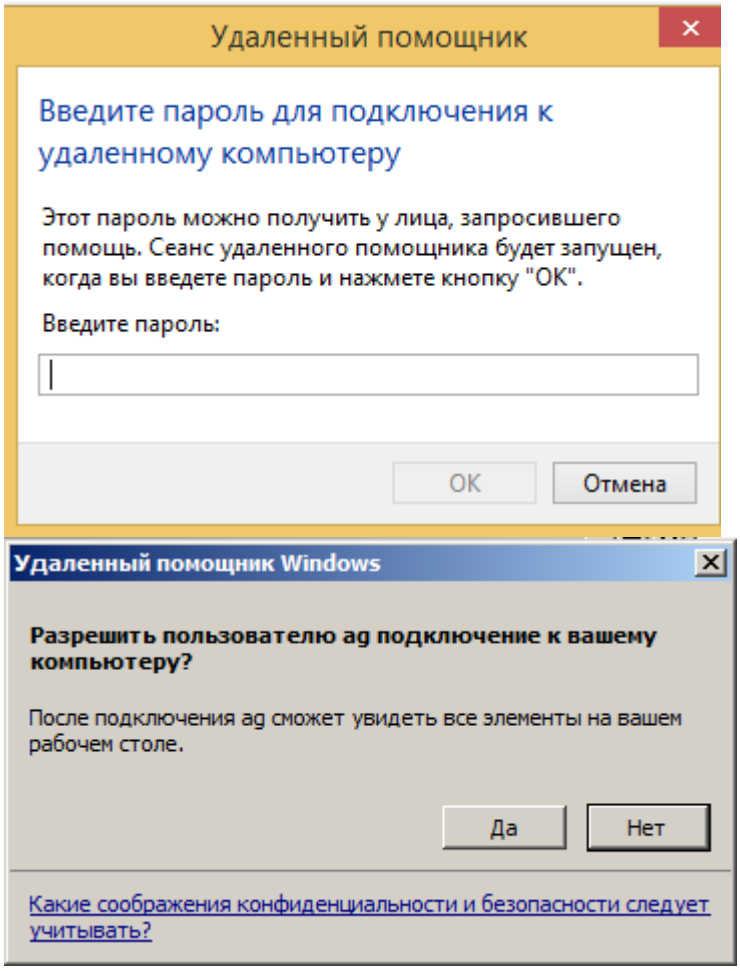


Отправка и получение сообщения

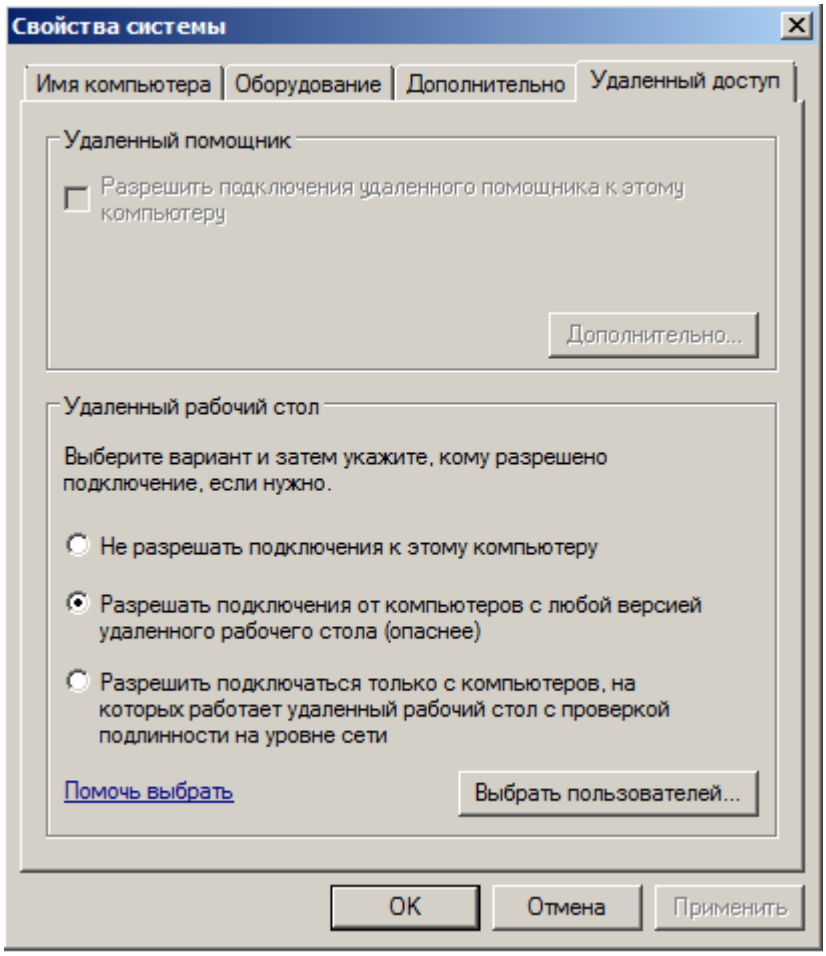
13. Настроить удаленного помощника
    a. Установить компонент **Удаленный помощник**.
    b. Создать **приглашение**. Сохранить приглашение как файл. Отправить файл и пароль соседу
    c. Подключить к соседу. Протестировать работу удаленного помощника. Протестировать режим чата (кнопка - разговор).







14. Настроить удаленный рабочий стол
    a. Включить удаленный рабочий стол.
    b. С помощью утилиты netstat проверить, что порт TCP 3389 “прослушивается”.
    c. Добавить локального пользователя в группу Пользователи удаленного рабочего стола (RemoteUsers).
    d. Подключиться к серверу соседа.
    e. Обнаружить пользователя в диспетчере задач в разделе Пользователи.



15. Настроить VNC
    a. Установить VNC-сервер. Licensekey: KRBAB-24NJY-8GCFB-ACD6Y-SKZ3A
    b. С помощью утилиты netstat –a –o –ptcp и диспетчера задач определить процессы и порты которые «прослушивает» vnc – сервер.
    c. Изучить опции VNC-сервера. Найти окно где задаются права доступа. Найти окно где задается порт.
    d. Найти в оснастке службы – службу VNCсервер. Изучить тип запуска и состояние службы.
    e. Найти в брандмауэре правила для VNC сервера.
    f. Подключиться к VNC серверу соседа.

16. Настроить TeamViewer
17. Оформить типовой отчет со скриншотами, для каждого ключевого пункта работы.

Часть 2. Выполнить в ОС семейства UNIX–Ubuntu

1. Настроить SSH
a. УстановитьopenSSH: sudo apt-get install ssh
b. Изучитьработукоманд: sudoservicesshstop|start|restart. Для чего они предназначены?
c. Подключиться к ssh-серверу соседа, используя ssh-клиент:
   sudosshимя_пользователя_соседа@ip_адрес_соседа
   Для правильности подключения проверяем:
   1. В настройках сети VirtualBox для ОС Ubuntu - Сетевой мост.

2. Проверяем настройки сетевого интерфейса (ваша машина с машиной соседа образуют одну подсеть).

d. Создать каталог в /home/имя_соседа/ сл. командой:
mkdirваша_фамилия
Создать текстовый файл в /home/имя_соседа/ сл командой:
sudonano newfile.txt
Выйти из ssh-клиента сл.командой: exit

e. Установить порт для ssh-сервера - 2020 (изменить порт используемый для ssh: в файле /etc/ssh/sshd_config - строка Port 22). Перезапустить ssh-сервер.

f. Подключиться к ssh-серверу соседа:
sudosshимя_пользователя_соседа@ip_адрес_соседа -p 2020
Удалить ранее созданный каталог, ранее созданный файл.
rmdirимя_каталога
rmимя_текстового_файла

2. Настроить VNC
a. Установить vncсервер
sudo apt-get install vnc4server
b. Изучить команду для управления vnc: vncserver
c. Запустить сервер
d. Установить vnc viewer
e. Подключиться к соседу

Контрольные вопросы

1. Для чего используются средства удаленного доступа и удаленного администрирования?
2. Какие средства удаленного доступа вы знаете?
3. Какой порт использует Telnetпо умолчанию?
4. Какой порт использует протокол RDP?

Лабораторная работа №11
Установка и настройка сетевых служб в UNIX, управление пользователями и правами доступа.

Цель работы: научиться устанавливать и настраивать сетевые службы в UNIX, научиться управлять пользователями и правами доступ

Компьютерная программа:программа VirtualBox с виртуальной машиной, с операционной системой семейства UNIX

Постановка задачи

Работа состоит из 3 частей.
В первой части необходимо установить и настроить DNS-сервер.
Во второй части необходимо установить и настроить DHCP сервер.
В третьей части необходимо создать пользователей, папки, и настроить права доступа.

Порядок выполнения

Работа выполняется в течении двух занятий.

Часть 1. Установить и настроить DNS сервер

1. Установить DNS-сервер BIND9
   sudo apt-get install bind9
2. Настроить файл /etc/resolv.conf (написать туда свой IP адрес (10.0.2.15))
3. Настроить сервера пересылки (forwarders). Файл: /etc/bind/named.conf.options
   - Указать DNS-сервера колледжа (10.7.2.1; 10.7.2.2)
   - Проверить работу кеширующего сервера утилитой dig. Два раза разрешить доменное имя и измерить время.
4. Создать и настроить зону прямого просмотра (фамилия.local).
   - Добавить запись (A) с именем www для веб-сервера (ip адрес придумать).
   - Добавить запись (CNAME) с именем web для веб-сервера.
   - Добавить запись (A) с именем ftp для ftp-сервера (ip адрес придумать).
   - Добавить запись (A) с именем mail для почтового сервера (ip адрес придумать).
   - Добавить запись (MX) для почтового сервера
     фамилия.local. IN MX 10 mail.фамилия.local.
   - Проверить конфигурационный файл зоны утилитой **named-checkzone**
     named-checkzon фамилия.local /etc/bind/db.фамилия.local
   - Проверить работу зоны утилитой **dig**
5. Создать и настроить зону обратного просмотра.
   - Проверить работу зоны утилитой **dig**.

Часть 2. Установить и настроить DHCP сервер

1. Установить dhcp сервер isc-dhcp-server
2. Создать пул ip адресов для раздачи. Настроить диапозон ip адресов. Настроить ip адрес dns-сервера. Настроить ip адрес шлюза.

Часть 3. Управление пользователями и правами доступа

1. Добавить 5 пользователей user1, user2, user3, user4, user5.

2. Добавить группы: group1, group2, group3.
3. Добавить:
user1 в group1;
user2 в group2, group3;
user3 в group1;
user5 вgroup2;
Замечание 1. Для добавления пользователя в группу, используйте:
$ sudo adduser username groupname

4. Удалитьпользователей user4, user5.
5. Открыть файл /etc/passwd, изучить структуру файла.
6. Открыть файл /etc/group, изучить структуру файла.
7. В своей домашней папке создать каталог directory.
Посмотреть права доступа для созданной папки:
$ ls -ld directory/

Удалить права чтения для всех:
$ sudo chmod 750 directory/

Посмотреть права доступа, что изменилось?
(/home - домашняя папка, mkdir folder_name - создать папку с именем folder_name).

8. Создатьпапки dir0,dir1,dir2,dir3,dir4.
Установить следующие права доступа для папок:
rwxrwxrwx для dir0;
rwxrwx--- для dir1;
rwxrwxr-- для dir2,
rwxrwxr-x для dir3,
rwx------ для dir4.

Контрольные вопросы

1. Что такое сетевые службы?
2. Как расшифровывается DNS?
3. Какие функции выполняет DNS-клиент?
4. Какие функции выполняет DNS-сервер?
5. Для чего используется утилита nslookup?
6. Можно ли организовать работу службы DNS автономно (без связи с сетью Интернет) ?
7. Для чего нужна зона прямого просмотра?
8. Для чего нужна обратная зона DNS?
9. Как работает рекурсивная схема разрешения имен?
10. Как работает не рекурсивная схема разрешения имен?
11. Как расшифровывается DHCP?
12. Режимы работы DHCP сервера?
13. Что такое DHCP-агент, зачем он применяется?
14. Алгоритм работы DHCP?

15. Как установить DNS-сервер BIND9?
16. Как тестировать и выявлять неисправности в работе DNS сервера bind9?
17. Назовите типы ресурсных записей?

Лабораторная работа №12
Диагностика и устранение неисправностей пассивного оборудования компьютерных сетей

Задачи

Часть 1..Определить места возможных неисправностей пассивного оборудования
Часть 2. Использование программных средств
Часть 3. Использование дополнительных (не входящих в состав компьютерной сети) инструментов и оборудования

Исходные данные/сценарий

В здании на нескольких этажах размещена компьютерная сеть организации. На каждом этаже организована горизонтальная подсистема сети на витой паре категории 5е. Горизонтальные подсистемы присоединены к мастер-кроссу витой парой SSTP категории 7а. От мастер-кросса организован выход к провайдеру сети Интернет по оптоволоконной паре с использованием медиаконвертера.
Цель первой части — определить, в каких элементах пассивного оборудования сети возможны неисправности. Перечислить такие элементы и их возможные неисправности. Обозначить, как активное оборудование информирует (сигнализирует) о неисправности пассивных элементов.
Во второй части лабораторной необходимо описать программные средства, средства операционной системы, утилиты командной строки для определения неисправностей пассивного оборудования.
В третьей части представить список инструментов для дополнительной проверки сетевого пассивного оборудования

Необходимые ресурсы

- 1 ПК (Windows 7, Vista или XP с выходом в Интернет)
- Дополнительно: калькулятор IPv4-адресов

Выполнение работы:

Часть 1: Определить места возможных неисправностей пассивного оборудования

В части 1 вам необходимо вспомнить состав пассивного оборудования сети:

Пример.
Патчкорд - отсутствие контакта в гнезде подключения к сетевой плате; отсутствие контакта в настенной розетке; обрыв.

Часть 2: Использование программных средств при определении неисправностей пассивного оборудования

В части 2 вам необходимо вспомнить программные средства диагностирования сети:

Пример.
При использовании команды ping происходит обмен ICMP - пакетами только с адресом 127.0.0.1, и не происходит обмен с другими известными адресами.

Часть 3: Использование дополнительных (не входящих в состав компьютерной сети) инструментов и оборудования

В части 3 вам необходимо перечислить средства диагностики сети и их возможности:

Пример.
Сетевой монитор - собирают данные о статистических показателях трафика, работают не только на физическом, но и на канальном, а иногда и на сетевом уровнях.

Вопросы на закрепление

Как влияет температурный режим помещения на работу пассивного оборудования?

Лабораторная работа №13
Диагностика и устранение неисправностей активного оборудования компьютерных сетей

Цель работы: Используя различные подходы к устранению неисправностей, выявить неисправности в активном сетевом оборудовании
Компьютерная программа: CiscoPacketTracer

Постановказадачиилиситуации:

В папке «problems»находятся файлы с топологиями сетей, для программы CiscoPacketTracer. В каждой топологии есть несколько неисправностей. Используя перечисленные ниже подходы поиска неисправностей, выявить «места» возникновения неисправностей, устранить неисправности.

Подходы к устранению неисправностей:

1. **Сверху-вниз**. Поиск неисправности по стеку OSI от уровня приложений до физического уровня. Эффективен если проблему наверху. (+) – чаще всего проблемы пользователей на прикладном уровне. (-) – нужен доступ к ПО пользователей.
2. **Снизу-вверх**. Снизу-вверх по модели OSI. (+) – поиск начинается с сети, и не нужно отвлекать пользователей. (-) – в крупных сетях трудоемко.
3. **Разделяй и властвуй**. Поиск с середины стека OSI (сетевой уровень) – утилитой ping. Далее решаете продвигаться вверх или вниз.
4. **Следуй пути**. Поиск неисправностей от источника к получателю. Диагностируются только устройства на пути.
5. **Поиск различий**. Сравнение конфигураций работающих устройств с проблемными.
6. **Перемещение проблемы**. Физически перемещать компоненты, и наблюдать движется ли проблема.

Основные этапы диагностики:

1. Сбор информации
2. Анализ информации. Сравнить симптомы с знаниями о системе, процессами в системе.Устранение возможных причин. Сравнение наблюдаемого поведения с ожидаемым может устранить причину.
3. Формулировка гипотезы.
4. Проверка гипотезы (решение на основе гипотезы, реализация решения).

Исходные данные

Имя файла	**Проблема**
problem_1	нет доступа с ПК0 к ПК5
problem_2	у ПК2, ПК3 нет IP адресов. (в сети 192.168.2.0/24 работает DHCP сервер)
problem_3	ПК0, ПК1 не имеют доступа к сайту ya.ru
problem_4	у ПК0 нет доступа к ПК5 (выявить неисправность, но не устранять)
problem_5	из подсети 192.168.1.0/24 нет доступа никуда
problem_6	в сети 192.168.2.0/24 у хостов нет доступа к сети (к другим

	сетям)
problem_7	компьютеры не могут открыть сайт site.com
problem_8	у User1, User2 не работает почта, они не могут отправлять почту друг другу

Порядок выполнения

1. Скопировать папку problems на свой компьютер.
2. Для каждого файла с проблемой – открыть, изучить формулировку проблемы, выбрать подход к устранению неисправностей, выявить неисправности, устранить неисправности.
3. Оформить отчет. Описать как искали неисправности – указать используемый метод. Описать гипотезы, которые были выдвинуты, какие из них были приняты? Какие вы опровергли? Если устранили неисправности – описать, что вы для этого сделали.

Контрольные вопросы

1. Назовите основные этапы диагностики неисправностей сети.
2. Перечислите существующие подходы к устранению неисправностей сети.
3. Назовите основные неисправности активного сетевого оборудования, с которыми вы столкнулись при выполнении лабораторной работы.
4. Опишите суть подхода «Сверху-вниз», его плюсы и минусы.
5. Опишите суть подхода «Снизу-вверх», его плюсы и минусы.
6. Опишите суть подхода «Разделяй и властвуй», его плюсы и минусы.
7. Опишите суть подхода «Следуй пути», его плюсы и минусы.
8. Опишите суть подхода «Поиск различий», его плюсы и минусы.
9. Опишите суть подхода «Перемещение проблемы», его плюсы и минусы.
10. Какие утилиты командной строки вы использовали при поиске неисправностей?

Лабораторная работа №14
Применение программных средства диагностики компьютерных сетей

Цель работы: Научиться использовать программные средства диагностики компьютерных сетей
Компьютерная программа:п рограммаVirtualBox с виртуальными машинами

Постановка задачи или ситуации:

Работа состоит из пяти частей. Первая часть посвящена работе с диспетчером задач. Вторая часть посвящена работе с системным монитором и счетчиками для сетевого интерфейса. Третья часть посвящена утилитам командной строки в операционной системе семейства Windows. Четвертая часть посвящена утилитам командной строки в операционной системе семейства UNIX. Пятая часть посвящена диагностическим утилитам в сети Интернет.

Порядок выполнения

Часть 1. Диспетчер задач

1. Открыть диспетчер задач, вкладку сеть.
2. Настроить View-> Update Speed -> Hight
3. В таблице должны присутствовать следующие столбцы: Adapter Description, Network Utilization, Link Speed, State, Bytes Sent Throughput, Bytes Received Throughput,Bytes, Bytes Sent, Bytes Received.
4. В отчет включить скриншот окна, описать поля (Adapter Description, Network Utilization…) - что они отображают?

Часть 2. Системный монитор. Сетевой интерфейс

1. Открыть оснастку Системный монитор.
2. Для сетевого интерфейса добавить следующие счетчики: Bytes Sent/sec; Bytes Total/sec; Current Bandwidth; Packets Sent/sec, Packets/sec.
3. Эмулироваить сетевую активность.
4. Просмотреть изменения счетчиков.
5. В отчет включить скриншот окна, описать добавленные счетчики. Описать, как и почему изменялись значения счетчиков во время эмуляции сетевой активности.

Часть 3. Выполнить в операционной системе семейства Windows
Для утилит, перечисленных ниже, выполнить требуемые действия.

ping (windows)

1. Вывести справку по команде
2. Выполнить ping узла по его IP адресу. Интерпретировать вывод утилиты.
3. Выполнить проверку узла до прекращения вручную (ping ya.ru -t)
4. Проверить связь с узлом 213.180.193.3 и сопоставить узел с узловым именем (т.е. узнать по ipадресу – имя узла).
5. Отправить 10 сообщений размером по 1000 байт (ping -n 10 -l 1000 10.0.99.221)

tracert (windows)

1. Вывести справку по команде

2. Выполнить трассировку маршрута до узла ya.ru. Интерпретировать вывод утилиты.
3. Выполнить трассировку пути к узлуya.ru и предотвратить разрешение каждого IP-адреса в имя (tracert -d ya.ru). Сделать вывод какой вариант трассировки работает быстрее и почему.
4. Выполнить трассировку к узлу ya.ruc количеством переходов равным 3. Сделать вывод по работе утилиты.

netstat (windows)

1. Вывести справку по команде
2. Выполнить команду, интерпретировать вывод.
3. Выполнить команду - показать таблицу маршрутизации (netstat -r)
4. Показать активные подключения с идентификаторами процессов (netstat -o)
5. Показать статистику интерфейса (netstat –s)
6. Вывести порты находящиеся в состоянии LISTENING (netstat -a | find "LISTENING")

nslookup (windows)

1. Вывести справку по команде
2. Разрешить имя
3. Разрешить IP адрес
4. Показать все записи типа MX для домена
5. Показать все записи типа SOA для домена

arp

1. Вывести справку по команде
2. Вывести arp таблицу (arp -a)

ipconfig

1. Вывести справку по команде
2. Вывести полную конфигурацию для всех адаптеров

Часть 4. Выполнить в операционной системе семейства UNIX
Для утилит, перечисленных ниже, выполнить требуемые действия.

ping (unix)

1. Вывести справку по команде
2. Выполнить ping узла. Интерпретировать вывод
3. Отправить 10 сообщений размером по 1000 байт (ping -c 10 -s 1000 ya.ru)

traceroute или mtr (unix)

1. Вывести справку по команде
2. Выполнить трассировку пути до узла. Интерпретировать вывод

netstat (unix)

1. Вывести справку по команде
2. Проконтролировать сетевые соединения. netstat –i
3. Отследить состояния сетевых соединений. netstat. + "прослушивающие" порты netstat –a
4. Узнать какие процессы на данном компьютере прослушивают сеть в ожидании входящих соединений. Идентифицировать прослушивающие сетевые службы netstat –l
5. Проверить таблицу маршрутизации. netstat –r
6. Просмотреть статистические данные функционирования различных сетевых протоколов. netstat -s

dig (unix)

1. Вывести справку по команде
2. Выполнить для домена. Интерпретировать вывод
3. Показать все записи типа A для домена (dig a ya.ru)
4. Показать все записи типа AAAA для домена (dig aaaa ya.ru)
5. Показать все записи типа NS для домена (dig ns ya.ru)
6. Показать все записи типа MX для домена (dig mx ya.ru)
7. Показать все записи типа SOA для домена (dig soa ya.ru)

nmap (unix)

1. Вывести справку по команде
2. Просканировать порты узла
3. Просканировать порты узла из диапазона 1-65535 (nmap p1-65535 192.168.1.1)
4. Просканировать порты узла и определить операционную систему (сделать для двух разных узлов) (nmap -O 192.168.1.1)

arp (unix)

1. Вывести справку по команде
2. Вывести arp таблицу (arp -n)

Часть 5. Диагностические сервисы

1. С помощью сервиса http://whatismyipaddress.com/ определить ваш IP адрес город, регион и страну.
2. С помощью сервиса http://www.whois-service.ru/ определить под управлением какого web-сервера работают сайты: vk.com;karelia.ru;ya.ru;wikipedia.com.
3. С помощью сервиса http://www.ip-1.ru/geocode/ узнать где находятся - karelia.pro, pkjt.karelia.ru, ya.ru, vk.com.
4. С помощью сервиса http://www.yougetsignal.com/tools/visual-tracert/ проследить путь до karelia.ru (по двум вариантам Host Trace, Proxy Trace). Сколько прыжков занимает путь? За какое время выполняется?

Контрольные вопросы

11. Назначение утилиты ping?
12. Назначение утилиты traceroute?
13. Назначение утилиты arp?
14. Назначение утилиты netstat?
15. Назначение утилиты nmap?
16. Назначение утилиты dig?
17. Назначение утилиты nslookup?
18. Назначение утилиты ipconfig?
19. Назовите наиболее распространенные варианты использования команды netstat в ОС UNIX?

Лабораторная работа №15
Применение плана действий восстановления работоспособности в реальной сети организации.

Необходимо иметь план на случай чрезвычайных обстоятельств. Каждый план должен иметь, как минимум, следующие разделы:

- Титульный лист. Официальное наименование плана, учетный номер, даты составления, изменений и утверждений, фамилии руководителей и исполнителей.

- Цель. Краткое описание целей составления плана, ЛВС, для которой он предназначен. "Основные положения" плана позволяют каждому, кто возьмет план в руки, быстро получить представление о нем.

- Общие стратегии. Приводится общее описание плана, а также:

* Процедуры первоначальной оценки ситуации и ввода плана в действие.

* Набор критериев, на основании которых объявляется бедствие.

* Перечень обязанностей сотрудников при восстановлении ЛВС.

* Общий перечень действий, выполняемых координатором восстановления ЛВС и другими ведущими сотрудниками.

* Общий перечень восстановительных работ, обеспечивающих либо организацию работы ЛВС в резервном центре, либо восстановление ее функционирования в производственном помещении, потерпевшем ущерб.

* Сводная оценка ущерба и сведения о необходимых работах по ремонту оборудования ЛВС.

* Время, требуемое на восстановление функционирования.

Учетная информация. Содержитразличные типы учетных данных. Например, стандартную конфигурацию сервера, стандартную конфигурацию рабочей станции, структуру каталогов, прочие данные о конфигурации, список идентификаторов, связанных с сервером, копии системных файлов для каждой рабочей станции, а также любые другие типы учетных данных, которые помогут осуществить восстановление ЛВС.

Состав группы восстановления после бедствия. Список всех лиц, которые будут принимать участие в восстановлении ЛВС, с указанием имени, домашнего адреса, телефона. В этот же список должны быть включены наименования, адреса и номера телефонов компаний-поставщиков услуг, оборудования.

Заблаговременные мероприятия. Список мероприятий, которые нужно проводить задолго до возникновения бедствия, чтобы уменьшить опасность его возникновения и возможные последствия.

Одним из таких важнейших мероприятий является **создание резервных копий**.

В плане должно быть указано, когда осуществляется создание резервных копий, куда они пересылаются, когда пересылаются, как должна выглядеть этикетка на носителях резервных копий и все то, что может потребоваться при реальном создании резервных копий.

Стандартизация этикеток и носителей облегчит работу тем, кто будет хранить копии, и тем, кому придется восстанавливать по ним информацию.

Данные на этикетках должны гарантировать, что носитель может быть легко доставлен из помещения с вашей ЛВС в место внешнего хранения и обратно и что им можно будет легко пользоваться.

Процедуры восстановления ЛВС. Требуемые действия в непредвиденных обстоятельствах и мероприятия по восстановлению функционирования ЛВС в различных ситуациях.

Рекомендации по правильному использованию материалов плана. Оставляем тут место для отметки о выполнении каждого этапа с указанием имени ответственного, даты и, возможно, времени выполнения.

Ведение плана. Этот раздел должен устанавливать процедуры ведения плана, в частности частоту корректировки соответствующей документации плана и лицо, ответственное за данное действие.

Даются рекомендации по составлению плановых документов, их рассылке и обучению методам составления и ведения плана. Если процедуры ведения определяются общими процедурами, установленными в компании, на них может быть сделана ссылка.

Испытания плана. В этом разделе описывается, что должно испытываться при проверке реализуемости плана, кто должен проводить испытания, когда должны осуществляться испытания и каковы их результаты.

План испытаний может быть общим или состоять из отдельных частей. Некоторые разделы этого плана могут являться разделами других общих планов.

Приложения. — Содержат различные формы, соглашения и т.п.

Приведенный нами вариант плана будет полезным для большинства ЛВС и не требует больших затрат на разработку, потому что может быть составлен с помощью обычного текстового редактора.

План создания резервных копий и восстановления информации в ЛВС

Регламенты резервного копирования могут различаться.

Целесообразно создавать полные резервные копии исходных текстов программ и критически важных приложений один раз в неделю, а инкрементное копирование — каждую ночь.

Производительность системы резервного копирования и восстановления информации не должна отставать от наращивания мощности вычислительных средств компании.

Несмотря на то, что конкретные регламенты резервного копирования и восстановления информации в разных компаниях различны, наличие четкого плана проведения соответствующих работ является необходимым.

В плане указываются: временные регламенты создания резервных копий, места хранения, вид этикеток на носителях и все, что может потребоваться при реальной работе, связанной с восстановлением данных. Стандартизация этикеток и носителей облегчит работу тем, кто будет хранить копии, и тем, кому придется восстанавливать по ним информацию. Данные на этикетках должны гарантировать, что носитель может быть легко доставлен из помещения с вашей ЛВС в место внешнего хранения и обратно и что им можно будет легко пользоваться.

Решающее значение при составлении плана имеет определение приоритетов. После анализа затрат следует проанализировать системные требования и задать приоритеты, учитывающие такие факторы, как объем и перечень имеющихся данных, для которых нужно создавать резервные копии. На основе проведенного анализа и заданных приоритетов распределяются ресурсы системы резервного копирования.

Реализация плана создания резервных копий должна быть повседневной заботой компании.

Зачастую неэффективность этого плана выявляется только тогда, когда происходит бедствие. Чтобы этого не случилось, необходимо регулярно проводить процедуры проверки типа "пожарных учений". Поскольку эти процедуры по восстановлению информации довольно трудоемки, для проведения их испытаний рекомендуется воспользоваться специальным программным обеспечением.

Лабораторная работа №16
Диагностика компьютерных комплексов и систем помощью диагностической программы AIDA 64.

Цель: изучить программное диагностическое средство AIDA 64 для определения работоспособного состояния ПК и устранения неисправностей.

1. Автоматизированный аудит сети

Точная инвентаризация ПК — это то, без чего невозможно обойтись в компании или организации. Управление инвентаризацией обновлений аппаратного и программного обеспечения всего компьютерного парка на бумаге или даже в электронных таблицах Excel требует существенных затрат труда и времени даже для небольших предприятий, не говоря уже о крупных корпорациях с сотнями и тысячами компьютеров.

Предлагаемая программой AIDA64 полностью автоматизированная инвентаризация сети снимает этот груз с плеч ИТ-специалистов. AIDA64 Business и AIDA64 Network Audit, предназначенные для бизнес-пользователей, позволяют выполнить подробную инвентаризацию аппаратного и программного обеспечения компьютеров на базе Windows, подключенных в одну корпоративную сеть. Объем информации, собираемый программой, можно полностью подстроить под требования пользователя, а администраторы получают возможность выбора между несколькими шаблонами (профилями отчета).

Рисунок 1 – Интерфейс программы AIDA64

2. Гибкостьконфигурации

Программа не требует установки, следовательно, ее можно запустить с общей центральной папки на любом клиенте в доменной среде. AIDA64 позволяет установить частоту создания отчетов (инвентаризации) компьютеров: отчеты можно собирать раз в месяц, раз в неделю, раз в сутки или после каждого входа пользователя в систему. Поскольку AIDA64 поддерживает параметры командной строки, процесс может быть полностью автоматизированным.

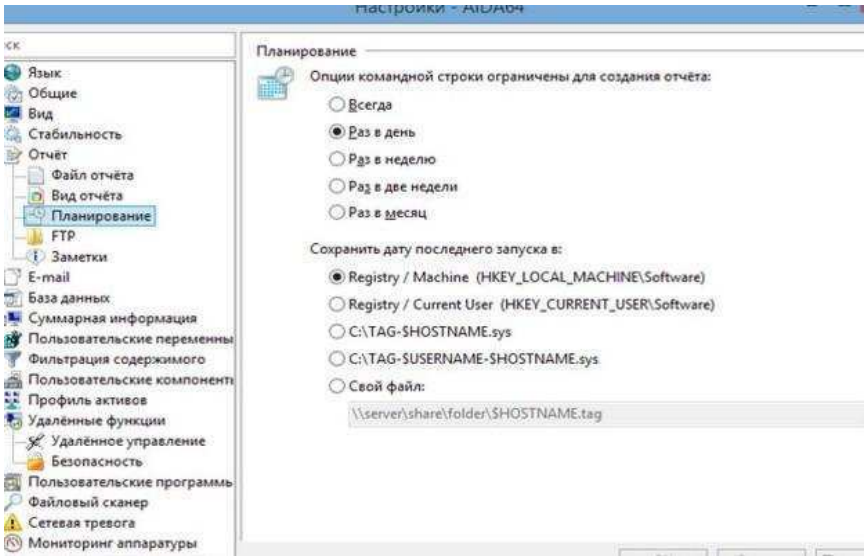


Рисунок 2 – Настройка отчётов AIDA 64

Отчеты можно сохранять в открытых форматах, готовых для дальнейшей обработки, а также в базе данных SQL. Версии AIDA64 Network Audit и AIDA64 Business поддерживают следующие форматы отчетов:

- обычный текстовый формат(TXT);
- HTML;
- MHTML;
- XML;
- CSV;
- MIF;
- INI;
- ADO (для вставки в базуданных).

3. Интегрированный администратораудита

Администратор аудита позволяет просматривать и анализировать инвентаризацию программного и аппаратного обеспечения компьютерного парка (рис.3). Здесь можно также отфильтровать данные и создать графики. Например, системные администраторы могут с легкостью определить клиентов, которые не отвечают минимальным системным требованиям новой применяемой программы, или для которых не установлены последние пакеты обновлений операционных систем и систем безопасности. В статистическом отчете (который можно отфильтровать по нескольким критериям), предоставляемом программой, можно сразу же увидеть процентное соотношение корпоративных компьютеров с определенным типом процессора, размером памяти илиустановленной версиейWindows.

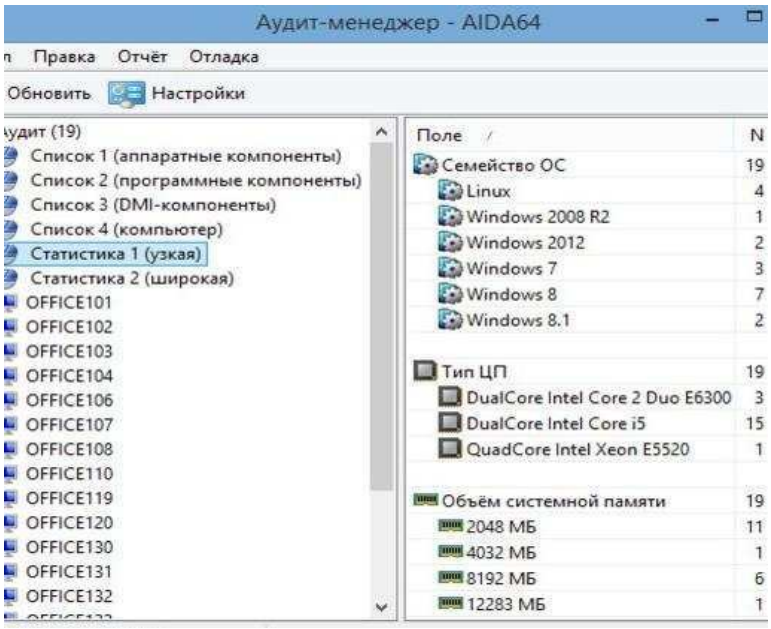


Рисунок 3 – Менеджераудита

Также можно отследить изменения между снимками сетевого аудита, сделанными в разное время, и обнаружить изменения в оборудовании или программной средекомпьютеров.

4. Управление изменениями и сетевоеоповещение

Интегрированное управление изменениями

AIDA64 Network Audit и AIDA64 Business позволяют отследить изменения между снимками сетевого аудита, сделанными в разное время (рис.4). Всего при помощи нескольких нажатий системные администраторы могут определить те компьютеры в корпоративной сети, конфигурация оборудования которых была изменена, или на которых установлено новое программное обеспечение, возможно, без разрешения. Можно также отследить, установлено ли на компьютере последнее обновление программ или операционной системы.

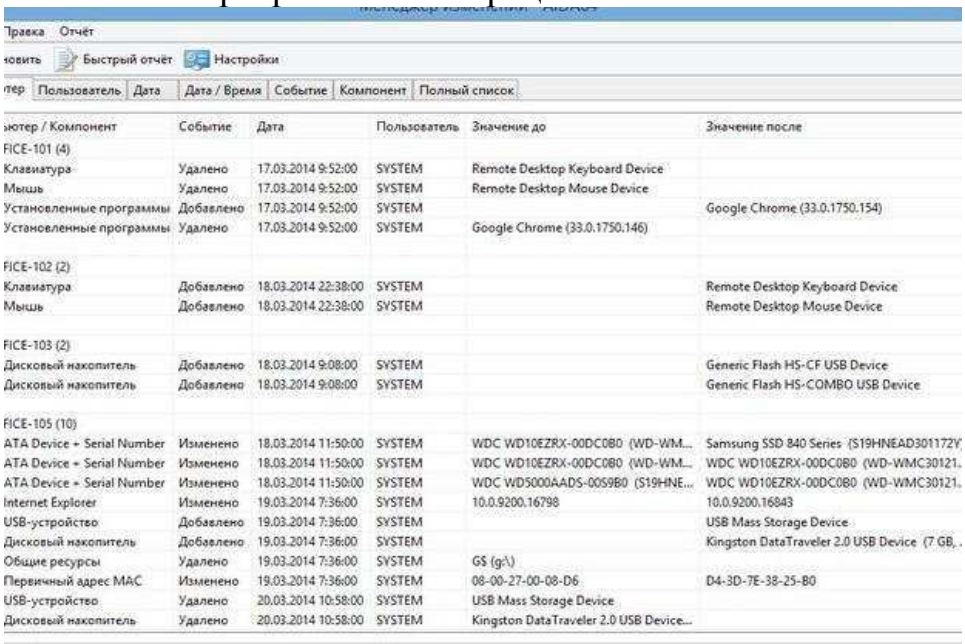


Рисунок 4 – Менеджер изменений

При помощи доступных файлов отчетов в формате CSV или SQL, функция AIDA64 Change Manager позволяет отсортировать изменения по пользователям, по

компьютеру, по дате, компоненту или событию, а также удалить некоторые выбранные компьютеры или пользователей из списка.

Мониторинг изменений в режиме реального времени

AIDA64 может отправлять оповещения в случае обнаружения изменений программного или аппаратного обеспечения или при возникновении каких-либо проблем (рис.5). Например, системные администраторы могут затребовать оповещения по электронной почте в случае, если пользователь подключает USB-накопитель к своему компьютеру, хотя не имеет на это права. При необходимости в подобных случаях специалист может даже вмешаться при помощи функции удаленного контроля.

AIDA64 поддерживает следующие виды инициации оповещений:

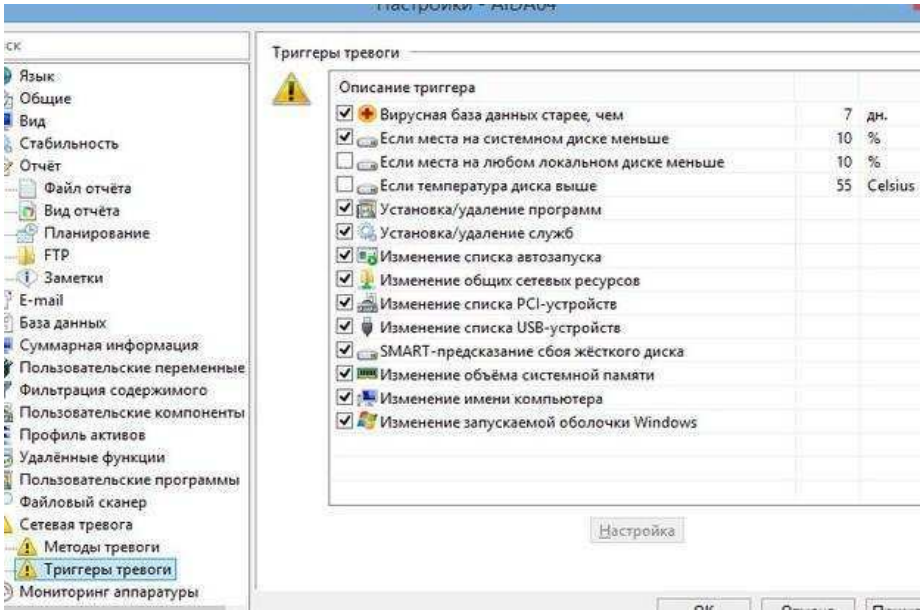


Рисунок 5 – Виды инициаций оповещений

При обнаружении события для оповещения, AIDA64 может отправить оповещение как пользователю, так и администратору несколькими способами, например, отобразив окно оповещения, отправив оповещение по электронной почте или сообщение Windows, или же записав событие в журнал (рис.6).

Данная функция поддерживается в следующих версиях:

- AIDA64 NetworkAudit;
- AIDA64Business.

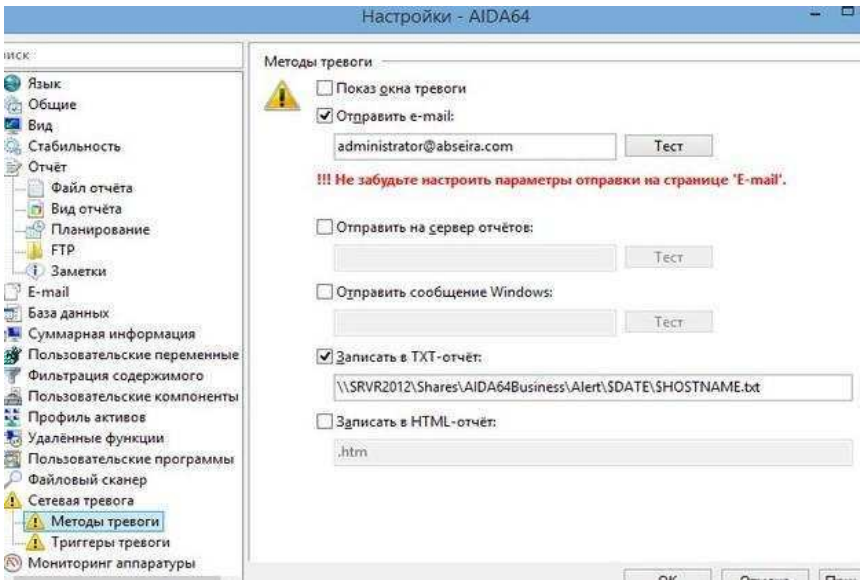


Рисунок 6 – Пример оповещения

Удаленный мониторинг иконтроль

AIDA64 Business предлагает расширенные функции удаленного контроля, которые позволяют системным администраторам отслеживать сетевую деятельность в режиме реального времени, проверять конфигурацию оборудования и программ на подключенных к сети ПК, а также полностью контролировать удаленные компьютеры, не покидая свое рабочееместо.

Мониторинг удаленных компьютеров

AIDA64 предоставляет в режиме реального времени информацию о компьютерах, подключенных к сети, которую, следовательно, можно использовать для мониторинга и контроля аппаратных ресурсов и использования сети (рис.7). Она сообщает системным администраторам о состоянии и работе каждого клиента; администраторы даже могут отследить количество работающих приложений и, имея должные на то полномочия, активные в данный момент окна, на которые смотрят пользователи.

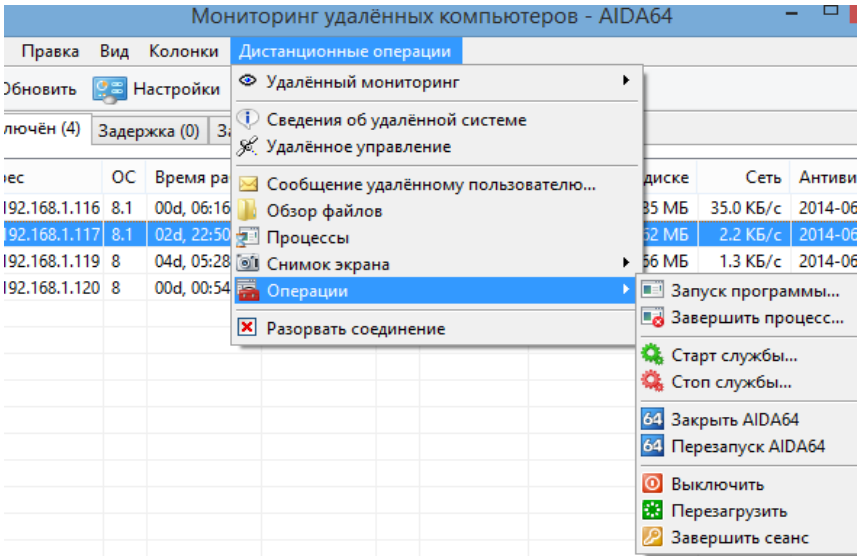


Рисунок 7 – Мониторинг удаленных компьютеров

Кроме мониторинга, программа также предлагает удаленные инструменты для вмешательства. Среди прочего, она позволяет администратору отправлять сообщения на удаленный компьютер или искать файлы, прекращать выполняемые процессы или делать снимки экрана. Такие функции можно использовать на всех

клиентах одновременно: например, если выбрать команду «Запустить программу» (Run program) в AIDA64 и набрать «Блокнот», Блокнот Windows откроется на всех компьютерах в сети.

Удаленная системная информация

AIDA64 Business также предоставляет подробную информацию о программном и аппаратном обеспечении на удаленных компьютерах в режиме реального времени. Во время сессии удаленного подключения можно увидеть подробные сведения об удаленной машине и просмотреть их в меню страницы и в информационномокне.

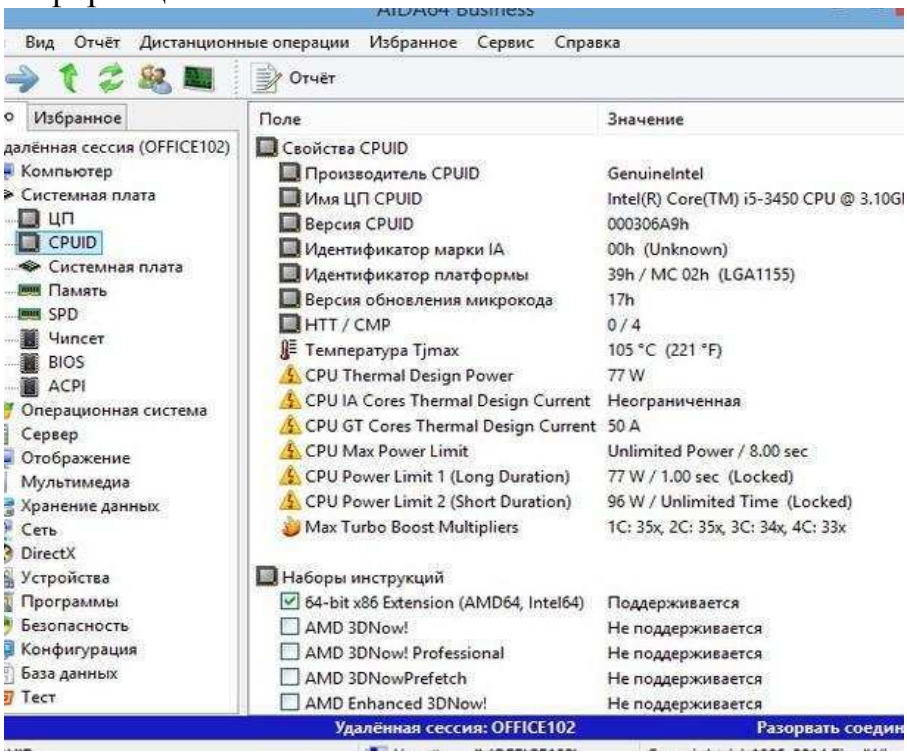


Рисунок 8 – Удаленное получение системной информации

5. Удаленный контроль

Администраторы также могут использовать эту программу для полного контроля удаленных компьютеров. Это может в значительной степени помочь в выполнении ежедневных административных задач, таких как поддержка, устранение неисправностей и обслуживание. Если у сотрудника, например, возникает проблема с офисным компьютером или приложением, администратор может предоставить удаленную поддержку, не покидая своего места.

AIDA64 Business позволяет выбрать те компьютеры, имена пользователей или IP-адреса, которые обладают полномочиями на установление удаленных подключений. Можно также установить защиту при помощи паролей для доступа к удаленным функциям, чтобы только уполномоченные пользователи могли их использовать.

AIDA64 Business всегда сообщает пользователям компьютера об установлении администратором удаленного подключения к их компьютеру.

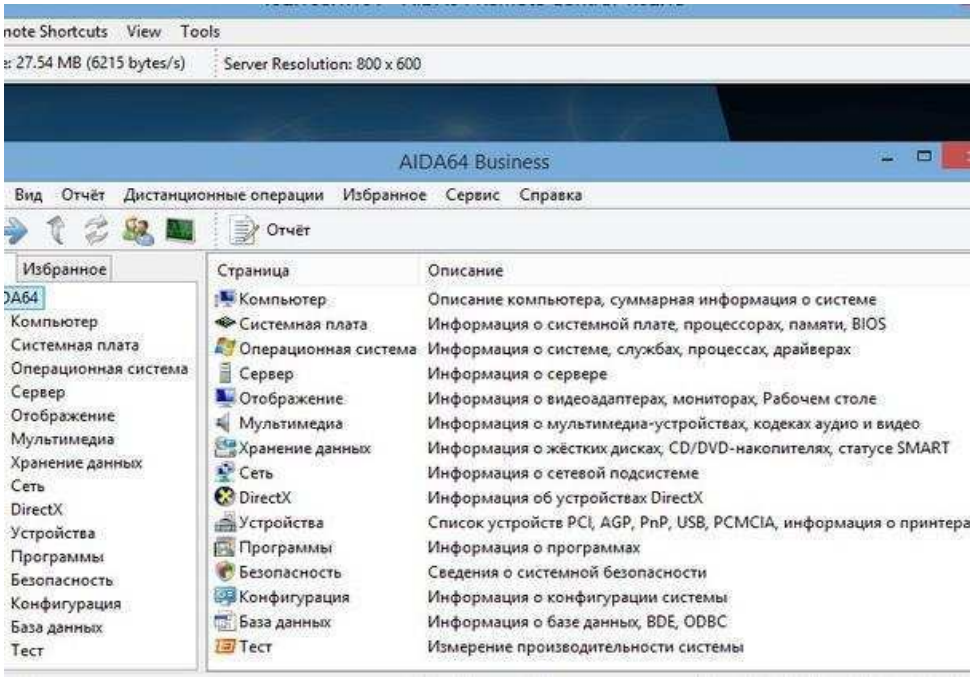


Рисунок 9 – контроль удалённых компьютеров

6. Обнаружениеоборудования

Программа AIDA64 обладает самыми точными функциями обнаружения оборудования в своем классе. Передовой механизм обнаружения оборудования основан на исчерпывающей базе данных оборудования, содержащей более 170 000 записей, что обеспечивает получение подробной и надежной информации о компонентах компьютера.

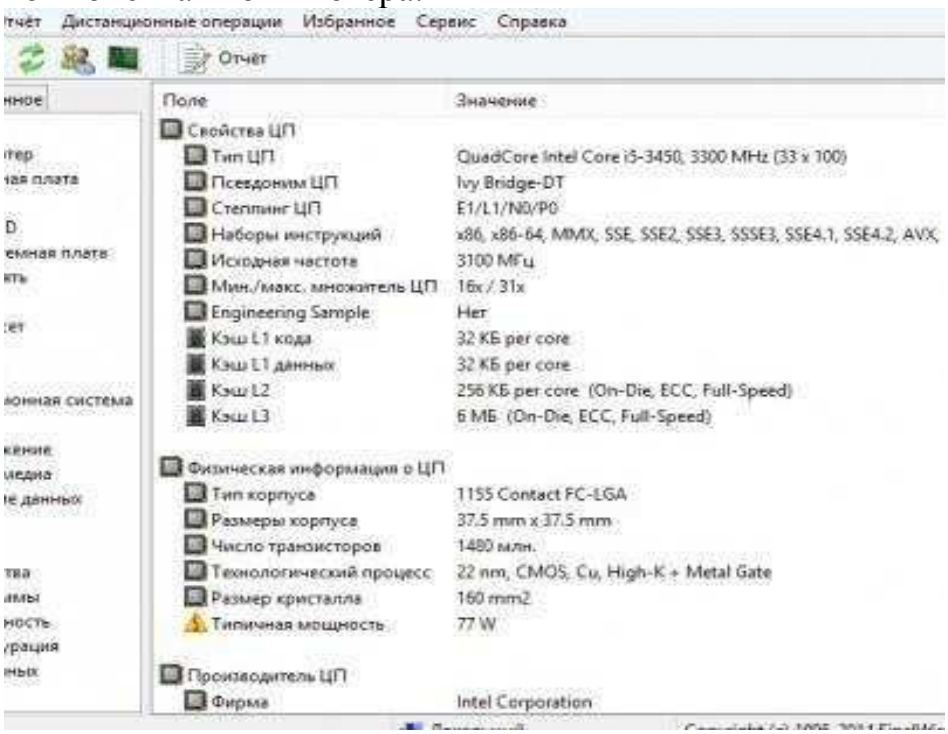


Рисунок 10 – Функция обнаружения оборудования

7. Тестированиепроизводительности

AIDA64 содержит несколько тестов, которые можно использовать для оценки производительности отдельных частей оборудования или системы в целом. Это

синтетические тесты, то есть они могут оценить теоретическую максимальную производительность системы. Тесты пропускной способности памяти, центрального процессора или FPU-блоков основаны на многопотоковом механизме тестирования AIDA64, который поддерживает до 640 одновременных потоков обработки и 10 групп процессоров (начиная с версии AIDA64 Business 4.00). Данный механизм обеспечивает полную поддержку для мультипроцессоров (SMP), многоядерных и гиперпотоковых технологий (рис.11).

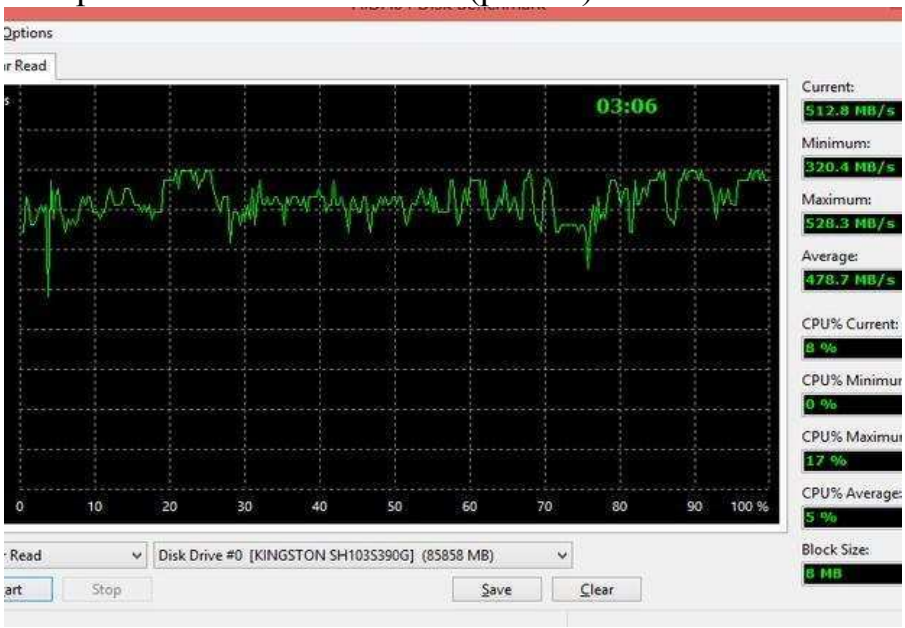


Рисунок 11- Тестирование производительности кэша и дисков

AIDA64 предлагает также отдельные тесты для оценки пропускной способности считывания, записывания и копирования, а также задержки кэша процессора и системной памяти. Также существует отдельный тестовый модуль для оценки производительности накопительных устройств, в том числе жестких дисков (S)ATA или SCSI, RAID-массивов, оптических дисков, SSD- накопителей, USB-накопителей и карт памяти.

Тестирование производительности GPGPU

Данная тестовая панель, доступ к которой можно получить в разделе меню Сервис Тест GPGPU, предлагает набор тестов производительности OpenCL GPGPU. Они разработаны для оценки вычислительной производительности GPGPU при помощи различных нагрузок OpenCL. Каждый отдельный тест можно выполнить максимум на 16 графических процессорах, включая процессоры AMD, Intel и NVIDIA, или их комбинации. Конечно же, полностью поддерживаются конфигурации CrossFire и SLI, а также dGPU и APU. В общем, данная функция позволяет протестировать производительность практически любого вычислительного устройства, которое представлено как графический процессор среди устройств OpenCL (рис.12).

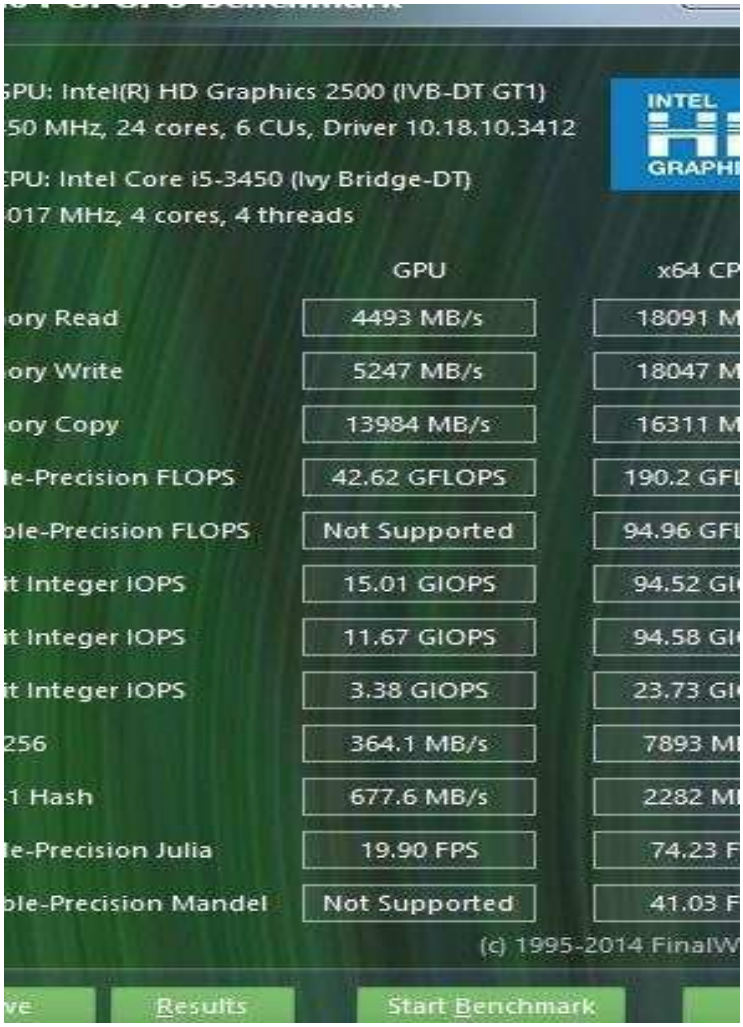


Рисунок 12 – Тестирование производительности

Кроме комплексных тестов производительности, AIDA64 предлагает специальные микротесты — их можно найти вразделе «Тесты» в меню «Страница». Благодаря исчерпывающей справочной базе данных результатов, результаты тестирования

производительности можно сравнить с аналогичными показателями по другим конфигурациям.

8. Тестирование производительностипамяти

Тесты производительности памяти оценивают максимально возможную пропускную способность при выполнении определенных операций (чтение, запись, копирование). Они написаны на языке ассемблера и максимально оптимизированы для всех популярных вариантов ядер процессоров AMD, Intel и VIA путем применения соответствующих расширений набора команд x86/x64, x87, MMX, MMX+, 3DNow!, SSE, SSE2, SSE4.1, AVX и AVX2.

Тест задержки памяти оценивает типичную задержку при считывании центральным процессором данных из системной памяти. Задержка памяти — это время для предоставления данных в регистре целочисленной арифметики центрального процессора после выдачи команды считывания.

9. Инструментальныймониторинг

Программа AIDA64 поддерживает более250 различных датчиков для измерения температуры, напряжения, скорости вращения вентилятора и потребления энергии (рис.13).

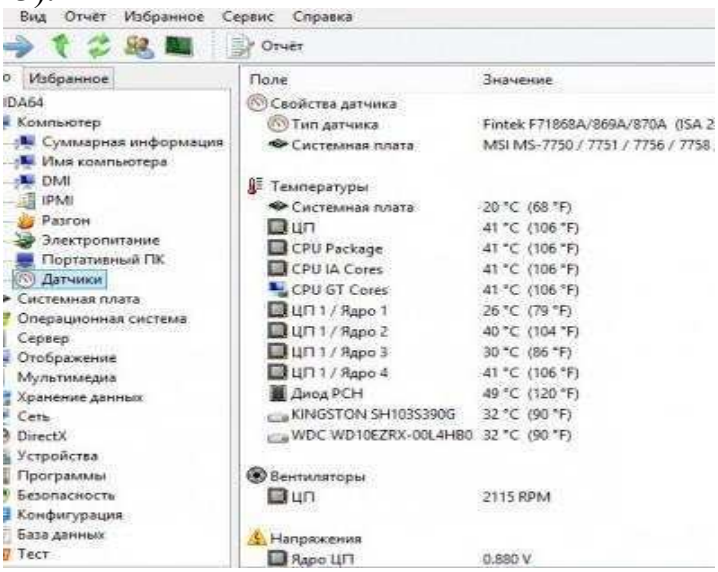


Рисунок 13 – Измерение температуры

Экранный мониторинг, оповещение

При помощи AIDA64 можно беспрерывно следить за состоянием компьютера, поскольку эта программа может показывать в режиме реального времени температуру, напряжение и скорость вращения вентилятора, измеряемые датчиками компьютера (рис.14). Если измеренные значения достигают критического уровня, например, когда вентилятор остановлен, программа оповещает об этом пользователя, или же сразу выключает компьютер.

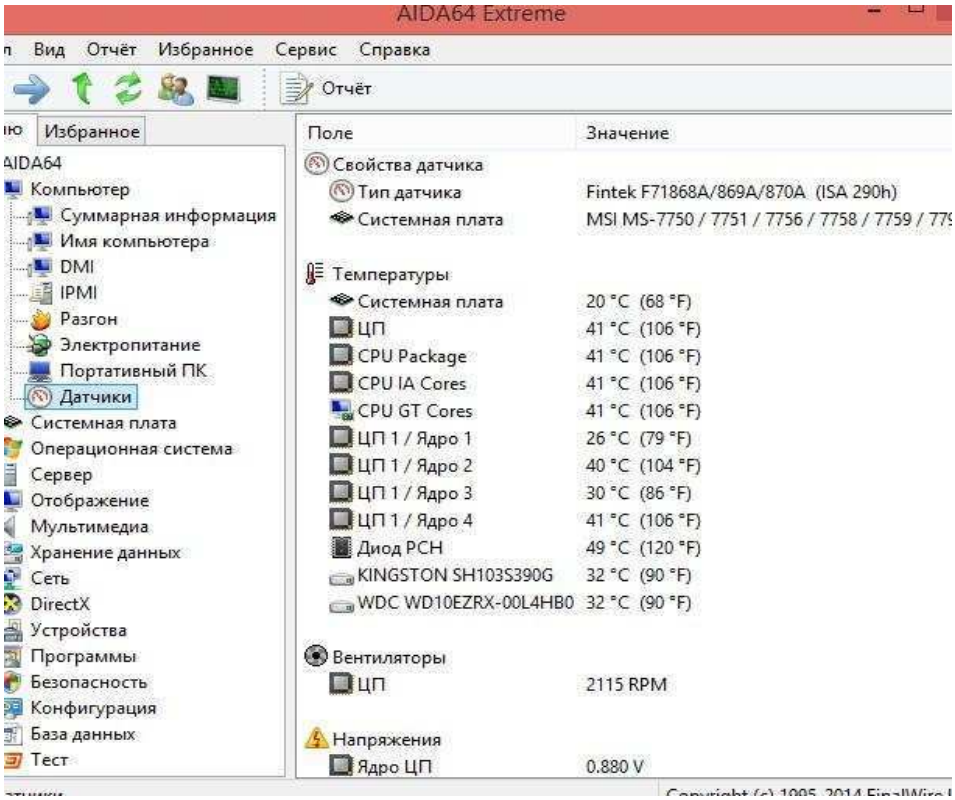


Рисунок 14 – Контроль важнейших характеристик

Существует несколько способов отображения программой AIDA64 измеренных датчиками показателей на рабочем столе Windows: на экранном дисплее, боковой панели гаджета, области пиктограмм панели задач, или на удобной настраиваемой графической панели SensorPanel (рис.15). Эта уникальная функция позволяет отобразить показатели измерений на LCD-дисплееигровой клавиатуры Logitech G15/G19, а также на LCD-дисплеях некоторых ноутбуков и клавиатур Razer. Показатели можно сохранить в файле HTML или CSV, а также экспортировать на внешние приложение, такое как RivaTuner или Samurai.

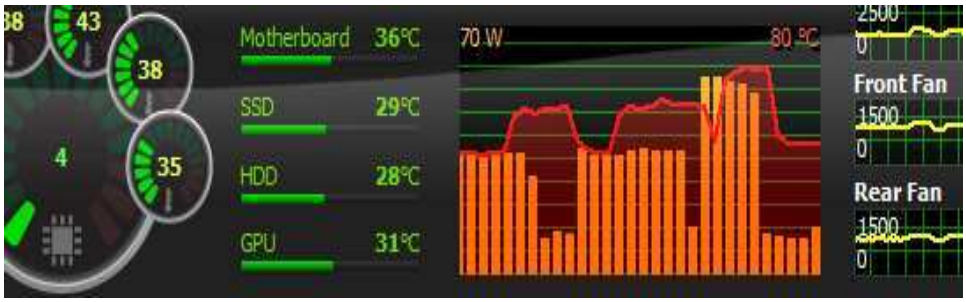


Рисунок 15 – Отображение информации на графической панели

AIDA64 может отправлять оповещения, когда показатели некоторых датчиков превышают установленные значения, например, если температура процессора достигает критических высот или если скорость вращения вентилятора охлаждения становится слишком низкой. Программа позволяет выбрать действия, которые она должна предпринимать при инициировании оповещения. В окне оповещения показаны доступные функции: выключение компьютера, воспроизведение

выбранного пользователем звука, запуск определенной программы или команды и отправка уведомления по электронной почте.

Данная функция поддерживается в следующих версиях:

- AIDA64Extreme;
- AIDA64Engineer;
- AIDA64Business.

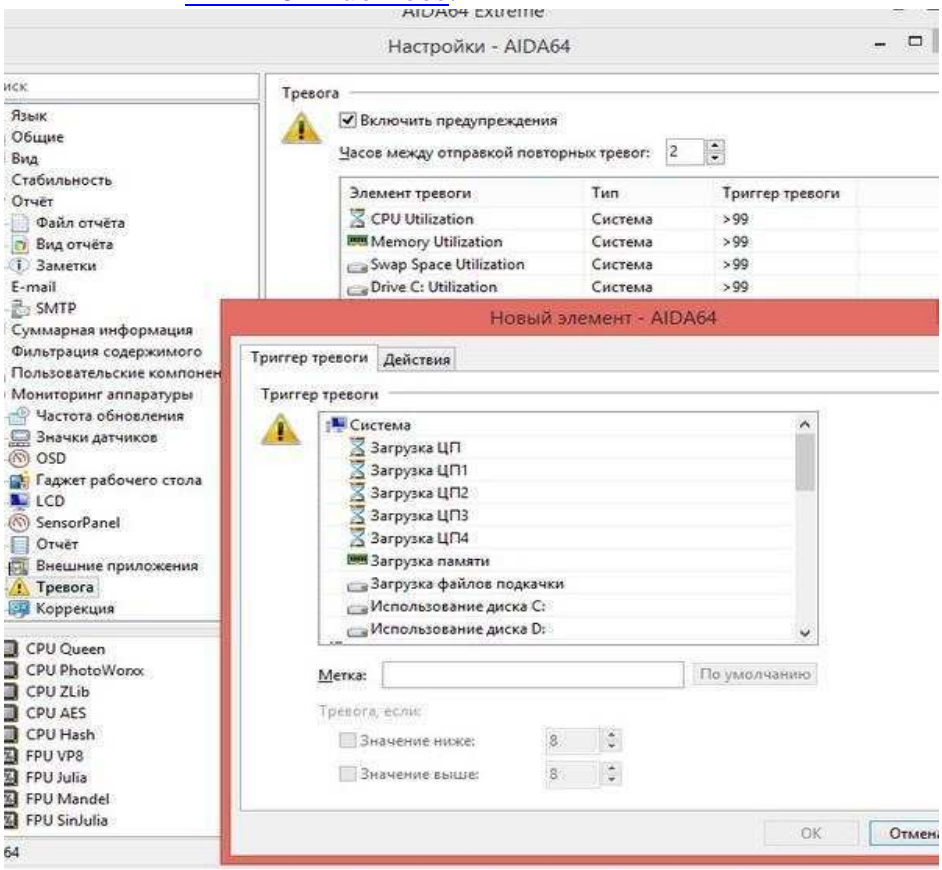


Рисунок 16 – Настройка способов оповещений

10. Информация о программномобеспечении

AIDA64 предоставляет невероятно подробную информацию не только об оборудовании компьютера, но и об операционной системе и установленных программах (рис.17). Она предоставляет перечень выполняемых процессов и служб, DLL- и AX-файлов, установленных обновлений Windows, плановых задач, установленных шрифтов и даже веб-страниц, которые пользователь открывал в Internet Explorer. Также предоставляется статистика продолжительности работы Windows и ошибки «синийэкран».

Существует возможность изменения некоторых настроек, связанных с программным обеспечением. В частности, можнозапускать или останавливать процессы, очистить историю браузера или удалить некоторые программы из списка автозапуска — и все это при помощи AIDA64, без запуска внешнего приложения.

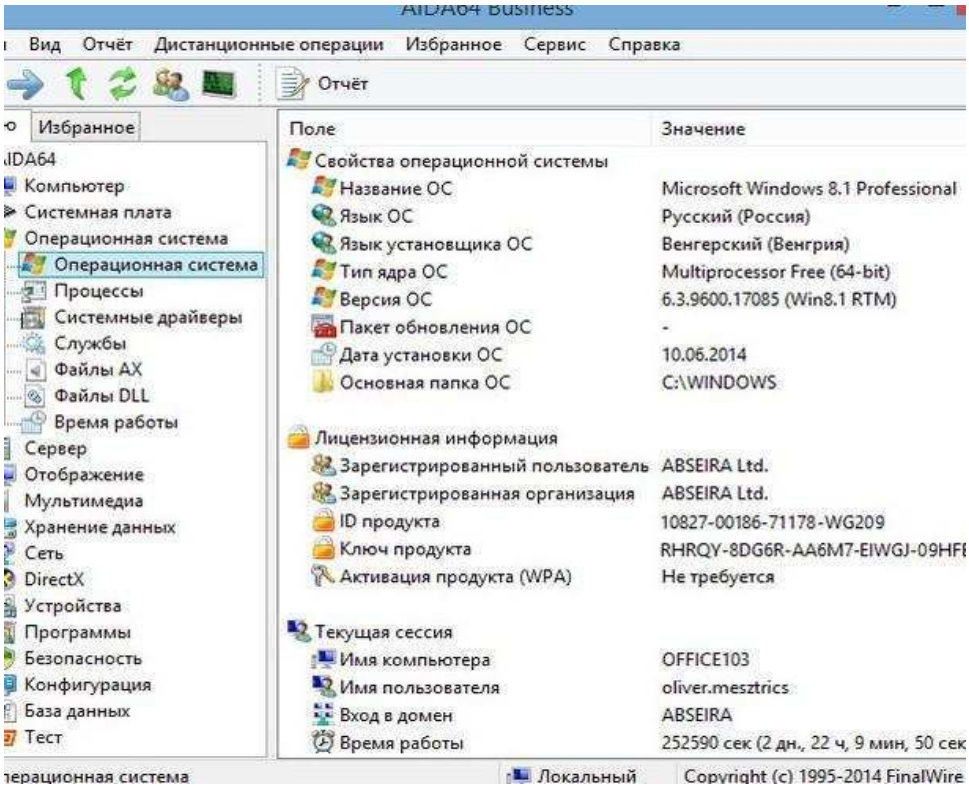


Рисунок 17 - Информация о программном обеспечении

Функция сканера файлов позволяет осуществить сканирование клиента по определенному расширению файла и сохранить перечень таких файлов в отчете. Например, если системный администратор хочет проверить, хранятся ли какие-либо файлы мультимедиа на корпоративных компьютерах, то при помощи AIDA64 можно составить такой перечень несколькими нажатиями кнопки мыши. Подобным образом можно проверить, доступны ли некоторые файлы и папки на клиентских компьютерах. Среди прочего, такая функция может быть полезна при отслеживании приложений, которые ввиду некоторых причин не показаны в перечне установленных программ в Windows.

Кроме этого, программа может составить список всех переменных среды, доступных в Windows, и создать журнал событий, где можно отсортировать информацию при помощи различных фильтров.

Данная функция поддерживается в следующих версиях:

- AIDA64Extreme;
- AIDA64Engineer;
- AIDA64 NetworkAudit;
- AIDA64Business.

Автоматические отчеты

Поддержка функций командной строки обеспечивает гибкость программы AIDA64 для создания автоматических отчетов. Программа поддерживает несколько форматов отчетов (рис.18).

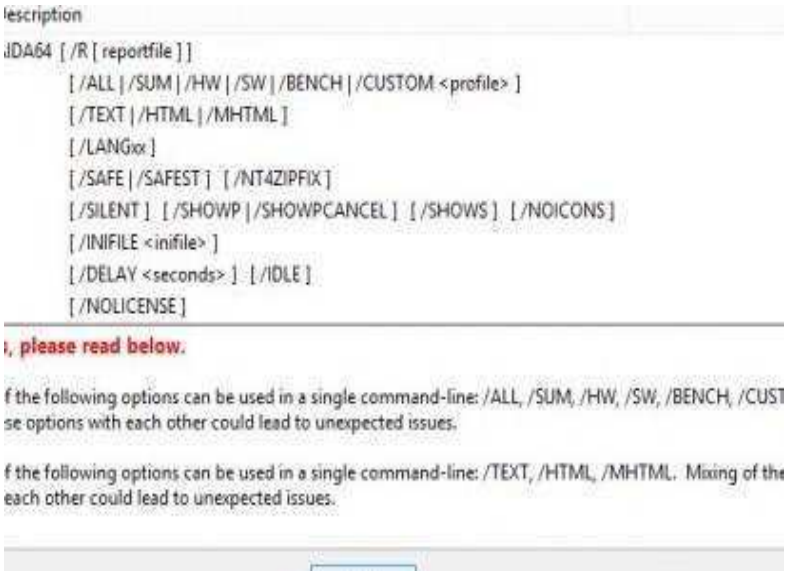


Рисунок 18 – Форматы отчётов

Практическое задание:

1. Проведите диагностику ПК и сети с помощью программы AIDA64.
2. По результатам выполнения диагностики сформируйтеотчёт, проанализируйте полученныерезультаты.
3. Ответьте на следующие контрольныевопросы.

Контрольные вопросы:

1. Для чего предназначена диагностическая программа AIDA64?
2. Как устанавливается программа для проведениядиагностики?
3. В каких форматах можно сформироватьотчёт?
4. Для чего предназначен администратораудита?
5. Поясните, как происходит управление изменениями и сетевое оповещение.
6. Какие виды оповещений используются впрограмме?
7. В каких версиях программы используется удаленный мониторинг иконтроль?
8. Как удаленно получить системнуюинформацию?
9. Удаленный контроль компьютеров с помощью программы AIDA64.
10. Обнаружение оборудования с помощью программы AIDA64.
11. Тестирование производительности и памяти с помощью программы AIDA64.
12. Инструментальный мониторинг ПК с помощью программы AIDA64.
13. Получение информации о программномобеспечении.

Лабораторная работа №17
Техническое обслуживание клавиатуры и манипулятора типа мышь

Цель: Изучить методику проведения ТО клавиатуры и манипулятора типа мышь.

Оборудование: ПК, клавиатура, манипулятор типа мышь.

1. Теоретическиесведения

1.1. Устройствоклавиатуры

Клавиатура предназначена для ввода алфавитно-цифровой информации и команд в ПК. Основой клавиатуры является матица контактов (клавиш). Клавиши могут выполняться в виде:

- резистивных датчиков, которые могут быть выполнены наоснове:
  - механическихконтактов
  - пленочныхконтактов
  - герконовыхконтактов
- емкостныхдатчиков

Задачу определения факта нажатия клавиши, формирование ее кода (скан-кода) и передачу данных в ПК решает специализированная микро-ЭВМ (контроллер клавиатуры). Структурная схема контроллера представлена на рис.2.

Основными элементами контроллера являются:

- Тактовый генератор
- Двоичный счетчик
- Дешифратр
- ПЗУ
- Селектор
- Выходной регистр

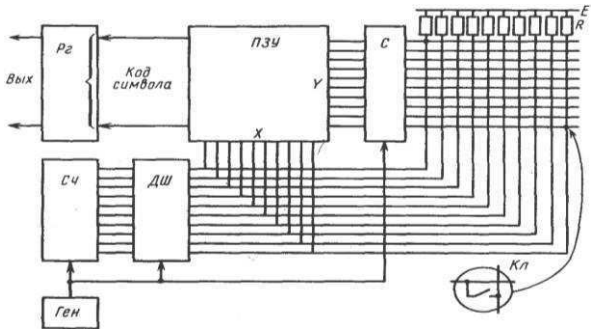


Рис. 1 Структурная схема контроллера клавиатуры

Связь клавиатуры с ПК осуществляется последовательным кодом.

1.2. Устройствомыши

Механическая мышь состоит из:

- стальной обрезиненныйшарик
- два пластмассовых валика сдисками
- микросхема управления с интерфейсом RS-232, PS/2, USB (в зависимости от мыши) иконтроллером
- ролик для скролинга(прокрутки)
- микровыключатели 2-3 шт. (в основном, хотя бывает ибольше)

Принцип работы мыши заключается в следующим: катая мышь по столу, мы перемещаем шарик, шарик касается валиков с дисками, через отверстия которых информация поступает на фотоприемники. Информация их фотоприѐмников обрабатывается в микросхеме управления и передается в ПК по последовательному интерфейсу. Мышь подключается к ПК 4-х проводным кабелем.

Основными элементами оптической мыши являются (Рис.2):

- Источник света (светодиод LED или полупроводниковый лазер)
- Оптическая система
- Светоприемник (Sensor)
- Мс обработки сигналов (Image Processor — процессор обработки изображений (DSP)).

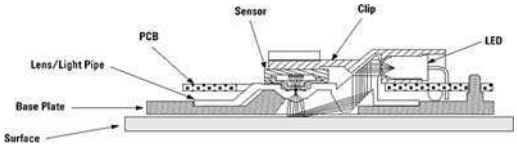


Рис. 2 Устройство оптической мыши

Принцип работы оптической мыши заключается в следующим: с помощью светодиода, и системы фокусирующих его свет линз, под мышью подсвечивается участок поверхности. Отраженный от этой поверхности свет, в свою очередь, собирается другой линзой и попадает на приемный сенсор микросхемы — процессора обработки изображений. Этот чип, в свою очередь, делает снимки поверхности под мышью с высокой частотой (кГц). На основании анализа череды последовательных снимков (представляющих собой квадратную матрицу из пикселей разной яркости), интегрированный DSP процессор высчитывает результирующие показатели, свидетельствующие о направлении перемещения мыши вдоль осей X и Y, и передает результаты своей работы вовне попоследовательному порту.

1.3. Профилактическое обслуживание клавиатуры имыши. Чистка клавиатуры

Чтобы поддерживать клавиатуру в рабочем состоянии, ее необходимо прочищать. Для профилактики рекомендуется раз в неделю (или хотя бы раз в месяц) чистить ее пылесосом. Вместо пылесоса для выдувания пыли и грязи можно использовать миниатюрный компрессор. Во время чистки с помощью

компрессора держите клавиатуру клавишами вниз.

Чистка манипулятора типа мышь

"Проскальзывание" механической мыши чаще всего происходит из-за того, что внутрь корпуса попали пыль и грязь.. Можно использовать кисточку или ватные палочки для прочистки нутра мышки, а с валиков спичкой удалить пояс из грязи. При этом
желательно не трогать оптическую систему: фото- и светодиоды. При их смещении мышь может оказаться неработоспособной.

Очень часто при эксплуатации, как механической, так и оптической мыши, по причине частого перегибания, происходит обрыв проводов в кабеле. Как правило, о такой неисправности говорит тот факт, что мышь то работает, то нет. Провода в кабеле обычно
обламываютсярядомскорпусоммышкиилирядомсеèразъèмом.Определитместообрывам ожноспомощьютестераилиспомощью шевеления кабеля одной рукой, а мышидругой.

При повреждении кабеля около корпуса мыши кабель отрезается на расстоянии примерно 5 см. от корпуса. Отпаиваем остаток старого кабеля и припаиваем новый.

Сложнееприповрежденииикабеляоколоразъèматаккаконнеразборный.Можновзя тькабельсразъèмом,скакой-нибудь мыши или поискать новыйразъèм.

2. Порядок выполненияработы:

2.1. Отключив клавиатуру и мышь от ПК выполнить последовательно основные сервисные процедуры для ТО клавиатуры имыши.
2.2. Запустив тестовую программу «Dr. Hardware 2007 English version» проверить правильность формирования клавиатурой кода нажатойклавиши.
2.3. Выполнить операции по прозвонки соединительного кабеля мыши. Используя условные обозначения зарисовать схему соединения разъемовкабеля.
2.4. Используя омметр проверить работоспособность кнопокмыши.

3. Контрольные вопросы изадания.

3.1. Каково назначение клавиатуры и манипулятора типамышь?
3.2. Каково назначение элементов контроллераклавиатуры?
3.3. Какова особенность организации интерфейса связи с ПК клавиатуры и манипулятора типамышь?
3.4. Каковы достоинства и недостатки основных типовклавиатуры?
3.5. Каков принцип работы оптическоймыши?
3.6. Каковы причины самопроизвольного перемещения указателя для оптическоймыши?

Лабораторная работа №18

Техническое обслуживание лазерных принтеров и их картриджей

Цель: Изучить методику проведения ТО лазерных принтеров и их картриджей. Освоить методику поиска неисправностей тракта формирования изображения.

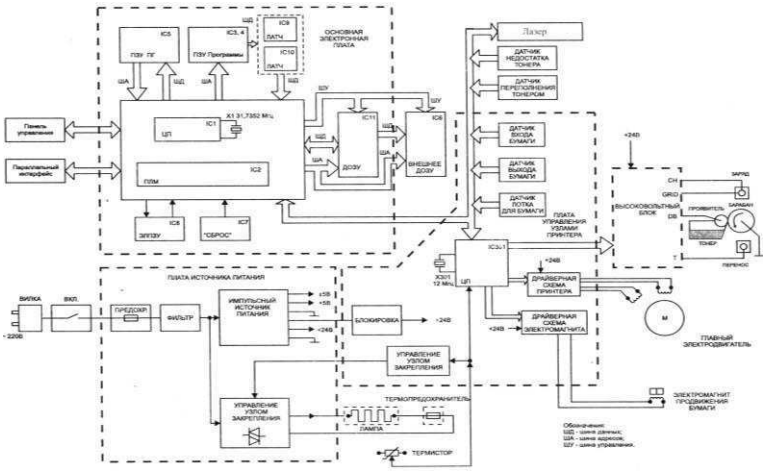
Оборудование: ПК, лазерный принтер.

1. Теоретическиесведения

1.1. Устройствопринтера

В основе работы лазерного принтера лежит электрофотографический принцип формирования изображения.

Суть этого принципа такова: источник света светит на предварительно заряженную поверхность *светочувствительного вала* (фотобарабана, фотовала). На тех местах, на которые попал свет, меняется заряд и к этим местам, затем притягивается тонер. Затем этот тонер перетягивается засчѐтэлектростатикинабумагу, накоторойпопадает в печку, где и закрепляется, под действием высокой температуры и давления.



Основными элементами принтера являются:

1. Основная электронная плата управления
2. Блок питания
3. Плата управления узлами принтера
4. Главный электродвигатель
5. Картридж
6. П/П лазер и схемасканирования
7. Фузер- электрическая печка

1.2. Профилактическое обслуживание принтера

Диагностика

Данные сервисные процедуры позволяют получить дополнительную информацию по диагностике принтера и выполнить мелкий ремонт.

Страница конфигурации (Self-Test)

Запуск данной страницы осуществляется однократным нажатием кнопки в

режиме готовности аппарата. Страница содержит основные настройки принтера, счетчик, модель, серийный номер, версии прошивки и языков, информацию об ошибках и опциях. Для запуска непрерывной печати страниц (для выявления проблем связанных с периодическим замятием бумаги) надо нажать кнопку на панели управления, включить принтер и удерживать кнопку в течение 5 с до загорания двух маленьких индикаторов, затем отпустить кнопку. Принтер будет печатать страницы конфигурации, пока в лотке есть бумага. Для остановки теста надо однократно нажать кнопку.

Чистка печки

Запуск данной процедуры осуществляется нажатием кнопки на панели управления в режиме готовности, и удерживанием кнопки в течение 10 с. После отпускания кнопки лист забирается, останавливается в печке, печка прогревается, и, через 4 с лист продвигается на ширину термоэлемента. Этот цикл повторяется до конца листа. На лист переходят остатки тонера с резинового вала и термопленки. В случае сильного загрязнения печки процедуру можно повторить еще 2–3 раза. Если грязь осталась и после этого, печку придется разбирать и чистить Уайт-спиритом, а в случае повреждения резинового вала или термопленки придется их заменить.

Engine Test

Данный тест позволяет произвести печать без участия платы форматера. Формирование конфигурационной страницы ведется с помощью форматера, поэтому если принтер не печатает с компьютера, и не печатает тестовую страницу, есть смысл проверить форматер. Запуск теста осуществляется нажатием кнопки на плате управления. Для получения доступа к кнопке достаточно снять левую крышку. Затем надо нажать кнопку тонкой отверткой, просунув последнюю в отверстие под форматером. При этом должна отпечататься страница с тонкими поперечными полосками. Эта страница формируется в плате ECU, и ее успешная распечатка означает исправность платы ECU. Если принтер не печатает с компьютера и свою страницу конфигурации, а печатает Engine Test, то неисправна платаформатера.

Половинный тест (Half-Self-Test)

Данный тест позволяет «отсечь» половину стадий ксерографического процесса, и определить в какой половине появляется дефект. Для его запуска надо начать печать конфигурационной страницы и, когда лист наполовину окажется под барабаном (приблизительно через 5 с после начала запуска двигателя), открыть переднюю дверцу, прервав процесс печати. Далее надо вынуть картридж и посмотреть на барабан. Если дефект (пропуск изображения, точки, различные пятна и т.д.) присутствует уже на барабане, то он вызван узлом лазер-сканера, высоковольтного блока или самого картриджа. Если на барабане дефекта нет, то он появляется на стадиях переноса или закрепления, и проверять надо соответствующие узлы.

Проверка вращения барабана (Drum Rotation Test)

Если барабан не будет вращаться по какой-либо причине (неисправность привода барабана, заклинивание ролика переноса, неисправность картриджа и пр.), то картридж не будет детектирован, и принтер не выйдет в готовность. Для проверки вращения барабана следует пометить положение барабана маркером на

его шестерне и, вставив картридж, включить принтер. После запуска двигателя нужно достать картридж и посмотреть на метку. Если метка осталась на месте, то барабан не вращался и необходимо устранить причину неисправности.

Сброс памяти NVRAM на начальные установки (NVRAM Initialization)

Данная процедура сбрасывает все установки на начальные (заводские). Для сброса необходимо нажать кнопку на панели управления, включить принтер и удерживать кнопку в течение 20 с. Когда все индикаторы загорятся необходимо отпустить кнопку и подождать пока загорится индикатор готовности. Следует учесть, что при этом сбросится серийный номер аппарата (Product Serial Number), номер форматера (Formatter Number), Service ID, Status Log, все счетчики, набор символов для ДОС на PC-8, формат на Letter, и другие параметры. Поэтому пользоваться этой процедурой надо только в случае необходимости.

Чистка роликов

Чистку резиновых роликов подающих, протягивающих, выходных лучше производить очистительно-восстанавливающей жидкостью Platenclene от фирмы AF. Состав жидкости размягчает резину и позволяет продлить срок жизни этих роликов. Никогда не следует использовать спирт или спиртосодержащие растворы (за исключением изопропилового спирта), они сокращают срок службы резины. В некоторых случаях при большом износе ролики и тормозную площадку придетсязаменить.

1.2.1.ДЕФЕКТЫ ПЕЧАТИ ЛАЗЕРНОГОПРИНТЕРА

Дефекты печати лазерного принтера обусловлены:
Окончание тонера
Естественный износ фотобарабана
Случайные дефекты на поверхности фотобарабана
Дефекты вала предварительного заряда
Дефекты магнитного вала
Дефекты чистящего лезвия
Дефекты дозирующего лезвия Дефекты уплотнительного лезвия

2. Порядок выполнения работы:

2.1. Используя видеофильм, ознакомится с методикой разборки лазерного принтера для ТО. Записать последовательность выполняемых операций.
2.2. Выполнить основные сервисные процедуры для диагностики принтера

2.2.1. Печать страницы конфигурации, используя полученные
- данные определить Количество напечатанных
- страниц напринтере
- Объем
  установленной
  памяти Разрешение
  принтера
  Режим работы принтера

2.2.2. Половинный тест (Half-Self-Test) для этого через 10-15сек после начала печати страницы конфигурации открыть крышку принтера, и вынут картридж, извлечь лист. Открыв защитный кожух фотобарабана проанализировать вид не закрепленного изображения и при наличии дефектов определить неисправный элемент.

2.3. <u>Отключить принтер от сети!</u>

2.4. Выполнить операции снятию картриджа лазерного принтера.

2.5. Разобрать картридж. Выполнить отчистку его от остатков тонера. Очистить отсек для отработанного тонера.

2.6. Выполнить замену элементов
- картриджа: Фотобарабана;
- магнитног
- о вала;
- чистящего
- лезвия;

дозирующего
лезвия;
уплотнительног
о лезвия;
Собрать картридж и проверить его работоспособность, выполнив тест проверки вращения барабана (Drum Rotation Test).

3. Контрольные вопросы изадания.

3.1. Каково назначение основных элементов принтера?

3.2. Указать расположение основных элементов картриджа принтера.

3.3. Какие меры безопасности необходимо соблюдать при ремонте и диагностике принтера и почему?

3.4. Каковы основные дефекты печати принтера и чем они обусловлены?

3.5. Как качество бумаги влияет на качество печати и почему?

Лабораторная работа №19
Диагностика и устранение неисправностей в программном обеспечении.

3.1 Цель лабораторной работы

Целью данной работы является получение практических умений работы с утилитами Нортона и сервисными программами для диагностики и обслуживания компьютера и обработки информации, размещенной на его дисках.

3.2 Задание на выполнение лабораторной работы

1) Ознакомиться с работой ДИСПЕТЧЕРА утилит Нортона, содержанием утилит Нортона, их назначением, форматами команд, системой подсказок и способами выполнения.

2) Получить информацию об ЭВМ и отобразить в отчете: тип компьютера, версия ОС, тип процессора и наличие сопроцессора, количество последовательных и параллельных каналов обмена данными, текущее состояние дисплея, объем памяти и т.д.

3) Выполнить контроль состояния системных ресурсов и загруженности процессора.

4) Оптимизировать расположение данных на диске с помощью утилиты Speed Disk.

5) Скопировать в рабочую директорию EVM несколько файлов с различными расширениями. Удалите файлы с заданными расширениями.

6) Выполнить восстановление удаленных файлов с помощью утилиты Unerase.

7) Выполнить проверку диска и восстановление поврежденных файлов утилитой NDD. Отчет проверки отразить в таблице.

8) Отформатировать дискету, сделав ее системной.

9) Получить информацию о логической структуре дискеты. Результаты представить в графической форме поразрядно.

3.3 Краткие теоретические сведения

NortonUtilities - это интегрированный набор программ, позволяющих находить и устранять различные ошибки компьютера, повышать его быстродействие, выполнять диагностику и профилактику сбоев.

NortonUtilities заблаговременно предупреждают о потенциальных проблемах, сокращают время простоя в аварийных ситуациях, восстанавливают потерянные данные и обеспечивают вас информацией о "внутренностях" компьютера, которая бывает полезна при установке нового аппаратного и программного обеспечения.

Программы, входящие в состав пакета NU, можно условно разделить на 4 группы:

1) Recovery - утилиты для восстановления информации на дисках:
   - *DiskDoctor (ndd.exe)* - автоматическое устранение некоторых дефектов на дисках;
   - *Unerase (Unerase.exe),Smartcan*- восстановление удаленных файлов и каталогов;
   - *Unformat (Unformat.exe)* - восстановление удаленных файлов и каталогов на диске после его форматирования;
   - *DiskEditor* - мощная утилитатеперь использует улучшенный режим восстановления(AdvancedRecoveryMode);
2) SPEED - утилиты для повышения скорости чтения/записи на диске:
   - *SpeedDisk (Speeddisk.exe)* - дефрагментирование записей на дисках;
   - *NortonCache, Calibrate, Ncache2*- создание в ОП специальной области (кэша), повышающей скорость чтения/ записи.
3) SECURITY - утилиты для защиты информации от несанкционированного доступа:
   - *DiskMonitor* - защищает диск от несанкционированной записи;
   - *DiskReet* - позволяет выбрать разные методы защиты данных от любопытного взгляда;
   - *WipeInfo* - для удаления конфиденциальной информации,
4) TOOLS - утилиты общего назначения:
   - *DiskTools* - необходима для восстановления дискет, а также позволяет сделать диск загрузочным;
   - *Image и Rescue* - создает диск спасения или страховочную копию данных;
   - *SysInfo и Ndiag* - информация о конфигурации и производительности данного компьютера**;**

- *DupDisk* - программа дублирования гибких дисков**;**
- *NCC* - помощь при настройке режимов работы аппаратуры компьютера**;**
- *FileFind* - в существующих файлах;
- *SafeFormat*- обеспечивает быстрое и безопасное форматирование;

Любую из программ NortonUtilities для Windows можно запустить через NortonUtilitiesIntegrator (ярлык находится на рабочем столе), в котором слева выбирается нужная категория программ, а справа запускается собственно программа.

Главными функциями NUforWindows являются:

- восстановление удаленных файлов (NortonProtection и UnEraseWizard)
- защитаотсистемныхсбоев (CrashGuard, Rescue Disk, Rescue Recovery Wizard)
- диагностикаиустранениенеполадок (Norton Disk Doctor, Norton WinDoctor)
- защита компьютера от вирусов (NortonAntiVirusSE)
- ускорениеработыкомпьютера (Speed Disk, Norton Optimization Wizard)
- очистка дискового пространства (SpaceWizard)
- обновление программного обеспечения (LiveUpdate, LiveUpdatePro)
- информация о компьютере (SystemInformation)

Проверка на наличие вирусов на компьютере

Датчик NortonAntiVirusSEScan программы NortonSystemDoctor регулярно проверяет систему на наличие вирусов. Этот датчик позволяет также запустить проверку на вирусы в любое время вручную:

1) запустить NortonSystemDoctor.

2) Нажать правой кнопкой мыши на датчик "Поиск вирусов" и выбрать из контекстного меню выбрать команду "Обновить".

Получить информацию о своей системе

Программа SystemInformation поможет быстро получить всю необходимую информацию по вашей системе (о версии BIOS, типе шины или процессора, наличии портов, видео и мультимедийных устройств и т.д.).

Она также производит сравнительное тестирование системы, дисков и мультимедиа, позволяя оценить быстродействие компьютера.

Обслуживание дисков

Основными операциями по обслуживанию магнитных дисков являются следующие: устранение дефектов на дисках, оптимизация размещения информации на диске с целью ускорения доступа к ней, чистка магнитных дисков от ненужной информации для высвобождения дискового пространства и, как следствие, ускорения доступа к информации.

Устранение дефектов на дисках

Имеющие место на магнитных дисках дефекты разделяют на логические и физические.

Логические дефекты заключаются в нарушении файловой структуры диска или содержимого системной области диска - загрузочной записи и таблицы размещения файлов. Причинами появления логических дефектов могут быть сбои в работе компьютера, неправильные действия пользователя пли деструктивные действия компьютерных вирусов. При этом возможно появление так называемых *потерянных кластеров* (недоступных ни из одной папки) или *совмещенных файлов* (имеющих общие кластеры). В результате логических дефектов может возникать замусоривание дискового пространства, иметь место невозможность доступа к элементам файловой структуры диска, неправильная обработка информации из-за взаимовлияния файлов.

Физические дефекты проявляются в невозможности правильного чтения и/или записи данных на отдельных участках магнитного диска из-за механических повреждений, неудовлетворительного качества или старения магнитного покрытия диска. Вовремя обнаруженные физические дефекты опасности не представляют, поскольку кластеры с дефектными секторами помечаются как дефектные и в дальнейшем не используются. Новые, по не обнаруженные физические дефекты могут привести к потере определенной части данных. Особенно опасны физические дефекты в системной части диска, так как при этом могут оказаться недоступными целые фрагменты файловой структуры.

Для поиска и устранения дефектов на магнитных дисках применяются специальные утилиты, получившие название *дисковых сканер-корректоров.* Среди таких утилит широкое распространение получили MicrosoftScanDisk, входящая в состав Windows 9x/2000, и NortonDiskDoctor из комплекта NortonUtilities. Утилиты имеют одинаковую схему рабо-

ты: сначала выполняется проверка файловой структуры диска для поиска и устранения логических дефектов, затем проводится проверка поверхности диска для поиска и устранения физических дефектов. Найденные цепочки свободных кластеров в соответствии с реакцией пользователя преобразуются в файлы или объявляются свободными. Совмещенные файлы могут быть переразмещены для разделения. При обнаружении физического дефекта расположенные на дефектном участке данные по возможности перемещаются в другое место. Естественно, при этом часть данных может оказаться утраченной.

В среде Windows 9x/2000 сканер-корректор MicrosoftScanDisk содержится в файле scandskw.exe, который размещается в основной папке операционной системы. Для запуска сканер-корректора MicrosoftScanDisk достаточно из главного меню Windows выполнить команду *Программы /Стандартные/Служебные программы/Проверка диска (ScanDisk) (Programs /Accessories /SYStemTools /ScanDisk).* В результате открывается стартовое окно сканер-корректора MicrosoftScanDiskДальнейший порядок работы со сканер-корректором MicrosoftScanDisk следующий:

1) в списке диалогового окна сканер-корректора выделяются диски, подлежащие проверке;

2) выбирается вариант проверки — *Стандартная (Standard)* или *Полная (Thorough*);

3) при выборе варианта полной проверки после нажатия кнопки *Параметры (Options)* уточняются параметры полной проверки (нужно ли проверять системную область и/или область данных);

4) нажатием кнопки *Дополнительно (Advanced)* открывается диалоговое окно *Дополнительные параметрыScanDisk (ScanDiskAdvancedOptions)* и выполняется настройка параметров;

5) нажатием кнопки Запуск (Start) инициируется начало проверки. Установка флажка *Исправлять ошибки автоматически (Automaticallyfixerrors)* означает автоматическое исправление обнаруженных ошибок сканер-корректором без выдачи запросов пользователю.

После окончания работы сканер-корректора появляется панель, отображающая отчет о результатах.

Снятие образа диска

Image делает "снимок" важной информации о файлах на диске -
этот процесс называется *снятием образа диска.* Образ диска используется различными программами Norton Utilities для восстановления удаленных файлов и воссоздания удаленных папок после случайного форматирования или при серьезных повреждениях диска. Два примера таких программ — это UnErase Wizard и UnFormat.

Программа Image сохраняет данные *загрузочной записи, таблиц размещения файлов (FAT), и корневого каталога.* Напомним, что *загрузочная запись* - первый физический сектор на дискете или первый логический сектор раздела жесткого диска. Он определяет архитектуру диска (размер секторов, размер кластеров и т.д.). На загрузочных дисках он также содержит программу, которая загружает операционную систему. Каждый логический диск включает загрузочную запись, которая хранит следующую информацию о логическом и физическом строении диска:

- число байтов на сектор;
- размер кластера (число секторов на кластер);
- число секторов на диске;
- число секторов на дорожку;
- число сторон диска;
- байт описания носителя.

Для загрузочных дисков загрузочная запись содержит также загрузчик программы, которая загружает операционную систему),

В *файловой системе FAT* таблица размещения файлов — это таблица в системной области диска, которая идентифицирует каждый кластер как свободный, занятый или запорченный. На диске всегда хранятся две копии FAT — на случай, если одна из них запортится. Структура FAT — главный метод обеспечения файлового сервиса в MS-DOS и Windows).

Корневой каталог является основой структуры хранения файлов логического диска. Корневой каталог содержит элементы каталога для хранимых на диске файлов и папок верхнего уровня) в файл данных образа (IMAGE.DAT). Кроме того, создается резервная копия предыдущей версии данных образа (файл IMAGE.BAK), которую

можно использовать при повреждении текущего файла IMAGE.DAT. Восстановление удаленных файлов без образа диска затруднительно, особенно если они сильно фрагментированы. Наличие образа диска обеспечивает большую сохранность данных и увеличивает шансы их восстановления.

При каждом добавлении, удалении или изменении файлов структура файлов на диске меняется. Поэтому необходимо регулярно снимать образ диска с помощью программы Image. Необходимо иметь текущий образ каждого жесткого диска в системе. Следует иметь ввиду, что Image можно запускать из сети, однако снятие образа сетевого диска невозможно.

Speed Disk автоматически создает и обновляет образ диска при его оптимизации. Таким образом, нет необходимости снимать образ диска непосредственно после запуска Speed Disk.

Датчик образа в программе Norton System Doctor проверяет время снятия образа и может быть настроен на автоматический запуск Image через заданный временной интервал.

Повышение быстродействия компьютера

Norton Optimization Wizard повышает быстродействие компьютера путем оптимизации нескольких критических компонентов Windows.

Файл подкачки в операционной системе Windows используется для временного хранения данных, что позволяет увеличить объем физической памяти компьютера (ОЗУ). По умолчанию Windows динамически изменяет размер файла подкачки в соответствии с меняющимися условиями в системе. Отрицательное воздействие на производительность компьютера оказывает фрагментация диска. Установив разумно минимальный размер файла подкачки, можно, во-первых, уменьшить или исключить совсем фрагментацию файла подкачки, и, во-вторых, замедлить естественный процесс фрагментации диска. Norton Optimization Wizard анализирует текущее состояние системы и устанавливает наиболее оптимальный минимум размера файла подкачки, а также перемещает этот файл на более быстрый жесткий диск (если он в компьютере не один).

SpeedStart - некоторые из существующих на сегодняшний день приложений очень сложны и громоздки. Иногда приходится терять немало времени только на ожидание их запуска. Norton SpeedStart изучает процесс загрузки приложений в память и оптимизирует его. Благодаря этой программе многие приложения загружаются гораздо быстрее.

Файлы реестра в операционной системе Windows - информация об аппаратной и программной конфигурации компьютера и его приложений хранится в специальной базе данных, которая называется реестр. Реестр является важнейшим компонентом, от которого зависит работоспособность Windows, и неверное хранение в нем данных может привести к ухудшению быстродействия компьютера. Norton Optimization Wizard упорядочивает структуру данных в реестре, ускоряя, таким образом, процесс поиска в реестре информации, необходимой самой системе и прикладным программам.

Технология LiveUpdate

Технология LiveUpdate корпорации Symantec, включенная в NortonUtilities, позволяет своевременно обновлять NortonUtilities и файлы описания вирусов. LiveUpdate использует модем или подключение в Internet для автоматической загрузки обновлений непосредственно из Symantec. Пользователям NortonUtilities эти обновления предоставляются бесплатно. Запустить LiveUpdate можно из программы NortonUtilitiesIntegrator, из меню "Утилиты" NortonSystemDoctor, а также из программной группы NortonUtilities в меню "Пуск".

Новая технология Symantec - LiveUpdate Pro - упрощает обновление прикладных программ и аппаратных драйверов при наличии подключения к Internet. Доступ к LiveUpdate Pro осуществляется через службу Norton Web Services. LiveUpdate Pro осматривает вашу систему, идентифицируя установленное на ней программное и аппаратное обеспечение, затем проверяет свою базу данных и предоставляет вам список доступных обновлений. Можно выбрать нужные обновления, после чего LiveUpdate Pro автоматически выгрузит их и сразу установит на ваш компьютер или сохранит на жесткий диск с тем, чтобы вы могли установить их сами в более удобное для вас время.

Дефрагментация диска

Процесс поиска и объединения фрагментированных файлов и папок называется *дефрагментацией*. Дефрагментатор дисков выполняет поиск фрагментированных файлов и папок на локальных томах. Фрагментированные файл или папка разделены на множество частей и разбрасаны по всему тому. Если том содержит много фрагментированных файлов и папок, системе требуется большее время для обращения к ним, поскольку приходится выполнять дополнительные операции чтения с диска их отдельных частей. На создание файлов и папок также уходит больше времени, поскольку свободное пространство на диске состоит из разрозненных фрагментов. Системе приходится сохранять новые файлы и папки в разных местах тома.

Дефрагментатор дисков перемещает разрозненные части каждого файла или папки в одно место тома, после чего файлы и папки занимают на диске единое последовательное пространство. В результате доступ к файлам и папкам выполняется эффективнее. Объединяя отдельные части файлов и папок, программа дефрагментации также объединяет в единое целое свободное место на диске, что делает менее вероятной фрагментацию новых файлов.

Время, необходимое для дефрагментации тома, зависит от нескольких факторов, в том числе от его размера, общего числа файлов, степени фрагментации и доступных системных ресурсов. Перед выполнением дефрагментации можно найти все фрагментированные файлы и папки, проанализировав том. Полученные сведения позволят узнать, как много фрагментированных файлов и папок содержит том, и решить, следует ли выполнять дефрагментацию.

С помощью программы дефрагментации можно преобразовать тома, использующие файловые системы FAT, FAT32 и NTFS.

3.4 Вопросы к защите лабораторной работы

1) Назовите основные возможности пакета сервисных программ NortonUtilities.
2) Причины появления и классификация дефектов дисков.
3) Что понимается под логической ошибкой файловой структуры?
4) Как восстановить удаленный файл с диска?

5) Как исправить нарушение структуры записей на диск?
6) Как провести диагностику диска?
7) Как оптимизировать размещение информации на диске?
8) Как ускорить доступ к информации?
9) Как изменить набор утилит, обрабатываемых оболочкой Norton?
10) Как получить справку по использованию утилит из пакета NortonUtilities?
11) Как получить совет по методике устранения «неисправностей на диске»?
12) Как получить информацию о компьютере и его внешних устройствах?
13) Как просмотреть информацию о системных областях диска MBR, BR, FAT, Rdir?

Лабораторная работа №20

Работа с антивирусными пакетами.

Цель: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидности вирусов, способах заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Получить навыки работы с антивирусным пакетом Kaspersky.

1. Теоретическиесведения

Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и "заражает" другие программы, а также выполняет какие-нибудь вредные действия (например, портит файлы или FAT-таблицу, "засоряет" оперативную память).

Для маскировки вируса действия по заражению других программ и нанесению вреда могут выполняться не всегда, а при выполнении определенных условий. После того как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает также, как обычно.

Тем самым внешне работа зараженной программы выглядит так же, как и незараженной.

Рассмотрим проявление наличия вируса в работе на ПЭВМ.

Все действия вируса могут выполняться достаточно быстро и без выдачи каких-либо сообщений, поэтому пользователю очень трудно заметить, что в компьютере происходит что-то необычное.

Некоторые признаки заражения:

- некоторые программы перестают работать или начинают работатьнеправильно;
- на экран выводятся посторонние сообщения, символы ит.д.;
- работа на компьютере существеннозамедляется;
- некоторые файлы оказываются испорченными ит.д.
- операционная система незагружается;
- изменение даты и времени модификациифайлов;
- изменение размеров файлов;
- значительное увеличение количества файлов надиске;
- существенное уменьшение размера свободной оперативной памяти ит.п.

Некоторые виды вирусов вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. Другие вирусы стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске.

Таким образом, если не предпринимать мер по защите от вируса, то последствия заражения компьютера могут быть очень серьезными.

2. Разновидности компьютерныхвирусов

Вирусы классифицируют по среде обитания и по способу воздействия. По

среде обитания вирусы подразделяются на следующиевиды:

- исполняемые файлы, т.е. файлы с расширением exe, com, файловые вирусы, которые внедряются главным образом в bat, но могут распространяться и через файлыдокументов;
- загрузочные, которые внедряются в загрузочный сектор диска или в сектор, содержащий программу загрузки системного диска;
- макровирусы, которые заражают файлы-документы и шаблоны документов Word иExcel.;
- сетевые, распространяются по компьютернойсети.

По способу воздействия (особенностям алгоритма) вирусы отличаются большим разнообразием. Известны вирусы-паразиты, вирусы-черви, вирусы-невидимки (стелс-вирусы), вирусы-призраки (вирусы-мутанты), компаньон-вирусы, троянские кони и др.

Чаще всего встречаются вирусы, заражающие исполнимые файлы. Некоторые вирусы заражают и файлы, и загрузочные области дисков.

Чтобы предотвратить свое обнаружение, некоторые вирусы применяют довольно хитрые приемы маскировки. Рассмотрим "невидимые" и самомодифицирующиеся вирусы.

"Невидимые" вирусы. Многие **резидентные вирусы** (резидентный вирус при инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращение операционной системы к объектам заражения и внедряется в них) (и файловые, и загрузочные) предотвращают свое обнаружение тем, что перехватывают обращения операционной системы к зараженным файлам и областям диска и выдают их в исходном (незараженном) виде. Разумеется, этот эффект наблюдаетсятольконазараженномкомпьютере-на"чистом"
компьютере изменения в файлах и загрузочных областях диска можно легко обнаружить.

Самомодифицирующиеся вирусы. Другой способ, применяемый вирусами для того, чтобы укрыться от обнаружения, - модификация своего тела. Многие вирусы хранят большую часть своего тела в закодированном виде, чтобы с помощью дизассемблеров нельзя было разобраться в механизме их работы. Самомодифицирующиеся вирусы используют этот прием и часто меняют параметры этой кодировки, а кроме того, изменяют и свою стартовую часть, которая служит для раскодировки остальных команд вируса. Таким образом, в теле подобного вируса не имеется ни одной постоянной цепочки байтов, по которой можно было бы идентифицировать вирус. Это, естественно, затрудняет нахождение таких вирусов программами-детекторами.

3. Методы защиты от компьютерныхвирусов

Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов. Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны такжеи как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя;

- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты отвирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств:

- копирование информации - создание копий файлов и системных областейдисков;
- разграничение доступа предотвращает несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиямипользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Программы-детекторы позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов. Эти программы проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов. Такая комбинация называется сигнатурой. При ее обнаружении вкаком-либо файле на экран выводится соответствующее сообщение. Многие детекторы имеют режимы лечения или уничтожения зараженных файлов. Следует подчеркнуть, что программы-детекторы могут обнаруживать только те вирусы, которые ей"известны".

Таким образом, из того, что программа не опознается детекторами как зараженная, не следует, что она здорова - в ней могут сидеть какой-нибудь новый вирус или слегка модифицированная версия старого вируса, неизвестные программам-детекторам.

Программы-ревизоры имеют две стадии работы. Сначала они запоминают сведения о состоянии программ и системных областей дисков (загрузочного сектора и сектора с таблицей разбиения жесткого диска). Предполагается, что в этот момент программы и системные области дисков не заражены. После этого с помощью программы-ревизора можно в любой момент сравнить состояние программ и системных областей дисков с исходным. О выявленных несоответствиях сообщаетсяпользователю.

Многие программы-ревизоры являются довольно "интеллектуальными" - они могут отличать изменения в файлах, вызванные, например, переходом к новой версии программы, от изменений, вносимых вирусом, и не поднимают ложной тревоги. Дело в том, что вирусы обычно изменяют файлы весьма специфическим образом и производят одинаковые изменения в разных программных файлах. Понятно, что в нормальной ситуации такие изменения практически никогда не встречаются, поэтому программа-ревизор, зафиксировав факт таких изменений, может с уверенностью сообщить, что они вызваны именно вирусом.

Программы-фильтры, которые располагаются резидентно в оперативной памяти компьютера и перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Некоторые **программы-фильтры** не "ловят" подозрительные действия, а проверяют вызываемые на выполнение программы на наличие вирусов. Это вызывает замедление работы компьютера.

Однако преимущества использования программ-фильтров весьма значительны - они позволяют обнаружить многие вирусы на самой ранней стадии.

Программы-вакцины, или иммунизаторы, модифицируют программы и диски таким образом, что это не отражается на работе программ, но тот вирус, от которого производится вакцинация, считает эти программы или диски уже зараженными. Эти программы крайне неэффективны.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Лучшей стратегией защиты от вирусов является многоуровневая, "эшелонированная" оборона. Рассмотрим структуру этой обороны.

Средствам разведки в "обороне" от вирусов соответствуют программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На переднем крае обороны находятся программы-фильтры. Эти программы могут первыми сообщить о работе вируса и предотвратить заражение программ идисков.

Второй эшелон обороны составляют программы-ревизоры, программы-доктора и доктора-ревизоры.

Самый глубокий эшелон обороны - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные. В "стратегическом резерве" находятся архивные копии информации. Это позволяет восстановить информацию при её повреждении.

Итак, одним из основных методов борьбы с вирусами является своевременная профилактика их появления и распространения. Только комплексные профилактические меры защиты обеспечивают защиту от возможной потери информации. В комплекс таких мервходят:

1. Регулярное архивирование информации (создание резервных копий важных файлов и системных областейвинчестера).
2. Использование только лицензионных дистрибутивных копий программныхпродуктов.
3. Систематическая проверка компьютера на наличие вирусов. Компьютер должен быть оснащен эффективным регулярно используемым и постоянно обновляемым пакетомантивирусных

программ. Для обеспечения большей безопасности следует применять параллельно несколько антивирусных программ.

4. Осуществление входного контроля нового программного обеспечения, поступивших дискет. При переносе на компьютер файлов в архивированном виде после распаковки их также необходимопроверять.

5. При работе на других компьютерах всегда нужно защищать свои дискеты от записи в тех случаях, когда на них не планируется запись информации.

6. При поиске вирусов следует использовать заведомо чистую операционную систему, загруженную сдискеты.

7. При работе в сети необходимо использовать антивирусные программы для входного контроля всех файлов, получаемых из компьютерных сетей. Никогда не следует запускать непроверенные файлы, полученные по компьютернымсетям.

Современные технологии антивирусной защиты позволяют защитить от вируса файловые сервера, почтовые сервера и сервера приложений. Например, антивирус Касперского для защиты файловых серверов позволяет обнаружить и нейтрализовать все типы вредоносных программ на файловых серверах и серверах приложений, работающих под управлением ОС Solaris, включая "троянские" программы, Java и ActiveX – апплеты.

В состав антивируса Касперского для защиты файловых серверов входят(рис.1):

- антивирусный сканер, осуществляющий антивирусную проверку всех доступных файловых систем на наличие вирусов по требованию пользователя. Проверяются в том числе архивированные и сжатыефайлы;
- антивирусный демон, являющийся разновидностью антивирусного сканера с оптимизированной процедурой загрузки антивирусных баз в память, осуществляет проверку данных в масштабе реальноговремени;
- ревизор изменений, Kaspersky Inspector, отслеживает все изменения, происходящие в файловых системах компьютера. Модуль не требует обновлений антивирусной базы: контроль осуществляется на основе снятия контрольных сумм файлов (CRC – сумм) и их последующего сравнения с данными, полученными после изменения файлов.

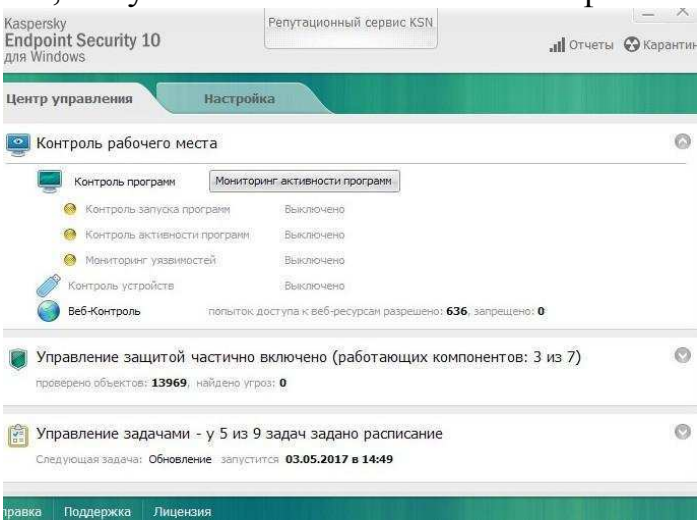


Рисунок 1 – Интерфейс антивирусной программы Касперский

Комбинированное использование этих модулей позволяет создать

антивирусную защиту, наиболее точно отвечающую системным требованиям.

Обнаруженные подозрительные или инфицированные объекты могут быть помещены в предварительно указанную "карантинную" директорию для последующего анализа.

Антивирус Касперского обеспечивает полномасштабную централизованную антивирусную защиту почтовых систем, работающих под управлением ОС Solaris.

Проверке на наличие вирусов подвергаются все элементы электронного письма – тело, прикрепленные файлы (в том числе архивированные и компрессированные), внедренные OLE-объекты, сообщения любого уровня вложенности. Обнаруженные подозрительные или инфицированные объекты могут быть вылечены, удалены, переименованы, или помещены в заранее определенную карантинную директорию для последующего анализа.

Ежедневное обновление базы вирусных сигнатур, автоматически реализуется через Интернет при помощи специально встроенного модуля и обеспечивает высокий уровень детектирования компьютерных вирусов.

Практическое задание:

1. Провести диагностику ПК и Вашей флешки с помощью антивирусной программы Kaspersky. Какие антивирусные программы установлены на вашем домашнемкомпьютере?
2. По результатом проведённой проверки составитьотчёт.
3. Ответить на контрольные вопросы (устно) при защитеотчёта.

Контрольные вопросы:

1. Что называется компьютерным вирусом?
2. Какая программа называется"зараженной"?
3. Что происходит, когда зараженная программа начинаетработу?
4. Как может маскироватьсявирус?
5. Каковы признаки заражениявирусом?
6. Каковы последствия заражения компьютернымвирусом?
7. По каким признакам классифицируются компьютерныевирусы?
8. Как классифицируются вирусы по средеобитания?
9. Какие типы компьютерных вирусов выделяются по способу воздействия?
10. Что могут заразитьвирусы?

Лабораторная работа №21
Создание хранилища на основе RAID

1. Какой из уровней RAID не обеспечивает избыточности?

Ответ:

2. Выход из строя любых двух дисков в RAID 10 группы не влияет на доступ к данным. Истинно или ложно?

Ответ:

3. Какой будет емкость массива RAID 10, если используются два диска по 2Тб, один диск 1,5 Тб и один диск 4 Тб?

Ответ:

4. Имеем RAID массив уровня 5, состоящий из 3-х дисков. В одном stripe на двух дисках содержится информация 00000000 и 11110000. Восстановите потерянную информацию для данного stripe на третьем диске.

Ответ:

5. Какие из следующих утверждений верны?
A. RAID - массив и физический том, построенный из нескольких дисков, одинаковы по функциональности.
B. Один логический том может быть создан на одном физическом томе.
C. На физическом томе можно создать несколько логических томов.
D. LUN может находиться в нескольких группах RAID

Ответ:

6. Для защиты от потери данных кэша RAID контроллера (сервера/системы хранения) в случае сбоя электропитания используется:

Ответ:

7. Какие из выражений о RAID 5 неверны?
A. RAID 5 имеет выделенный диск для данных контроля четности.
B. RAID 5 использует функцию XOR для контроля четности.
C. RAID 5 записывает данные блоками, размером, равным stripe.
D. RAID 5 обеспечивает отказоустойчивость без потери данных при отказе максимум двух дисков.

Ответ:

Задание:

1. Реализовать программный RAID 0 в Windows Server 2008
2. Реализовать программный RAID 1 в Windows Server 2008
3. Реализовать программный RAID 5 в Windows Server 2008

Лабораторная работа №22
Изучение возможностей архиваторов на примере pkzip, pkunzip, arj, WinZip, 7Zip.

Задание:
1. Установить архиваторы (7zip, Bandzip, FreeArc, HaoZip, WinRAR, WinZip).
2. Сжать аудио/видео/фото/текст. Размер исходных файлов должен быть не менее 50 Мбайт.
3. Сравнить (степень сжатия). Построить таблицу.

	7zip	Bandzip	FreeArc	HaoZip	WinRAR	WinZip
аудио						
видео						
фото						
текст						

4. Сделать многотомный архив
5. Сделать архив под паролем

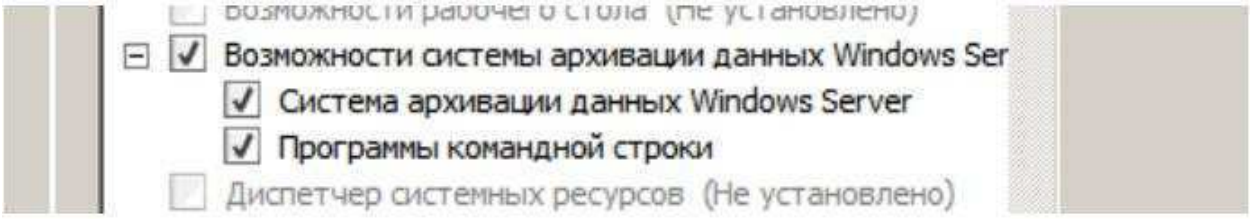
Лабораторная работа №23
Изучение возможностей программного обеспечения резервного копирования на примере Microsoft Ntbackup, Cobian Backup, Ascomp Backup Maker

Ход работы:

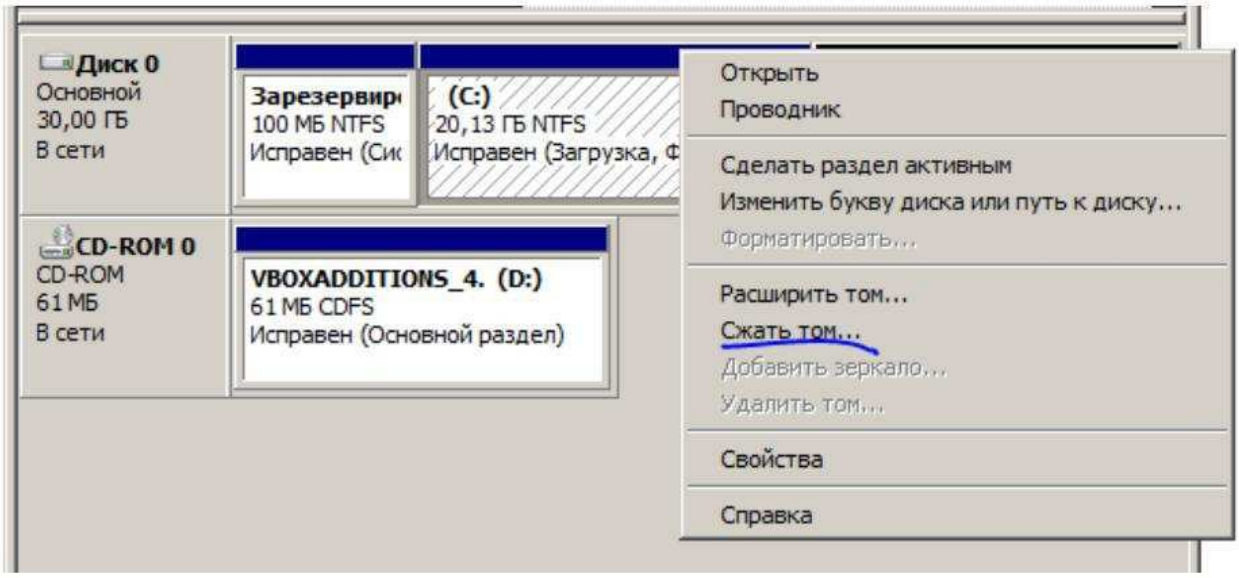
Часть 1. Microsoft Ntbackup

1. Изучить справку по работе со средствами резервного копирования Windows Server 2008 R2.

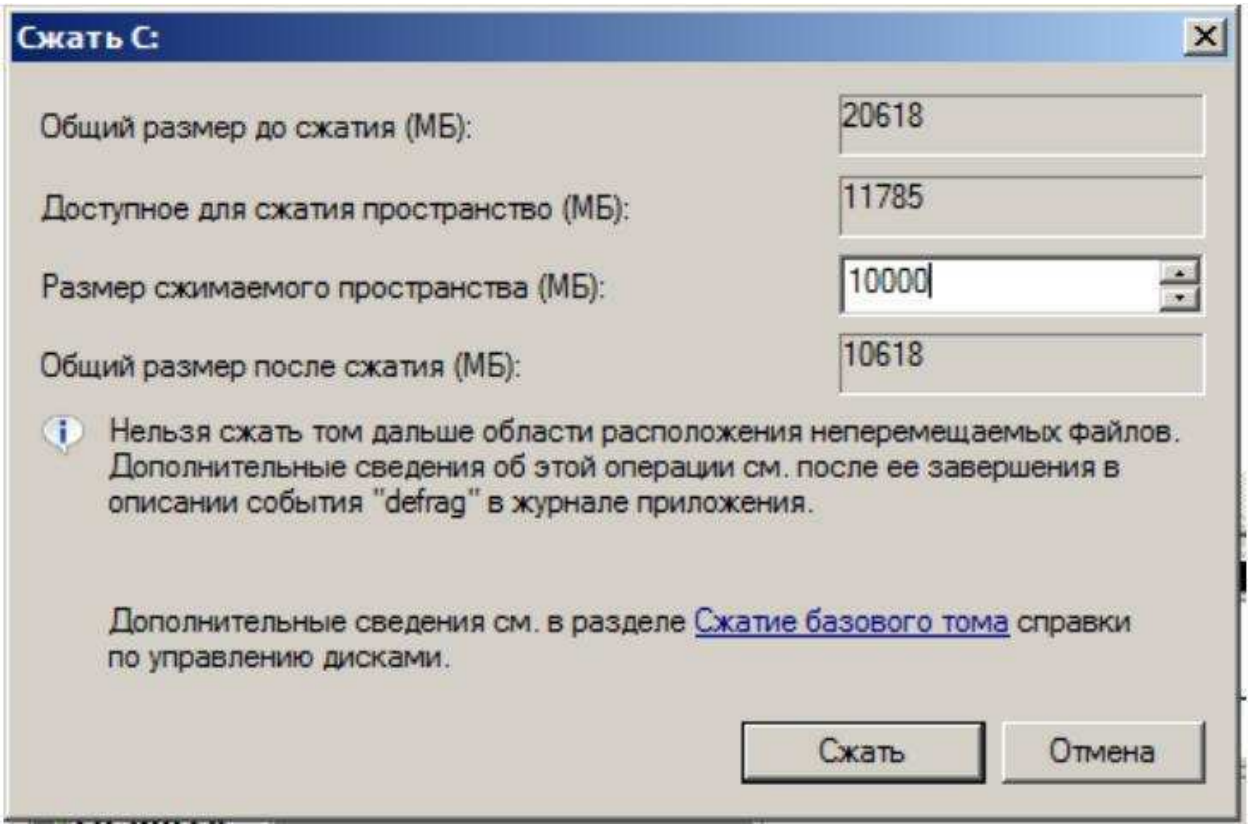
2. Установить компонент сервера “Возможности системы архивации данных Windows Server”. (Как найти: Диспетчер сервера->Мастер добавления компонентов->Возможности системы архивации данных Windows Server. Выбрать “Система архивации данных Windows Server”, “Программы командной строки” см. рисунок ниже)



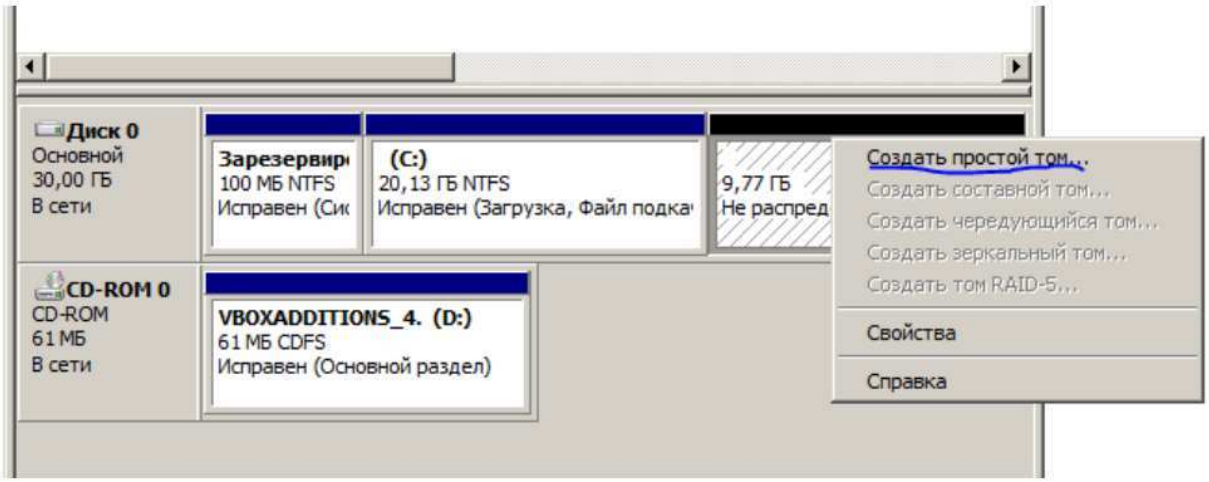
3. Создать новый диск, на котором будут хранится резервные копии. Для этого - открыть остнастку “Управление дисками”. Найти жесткий диск, сжать том.

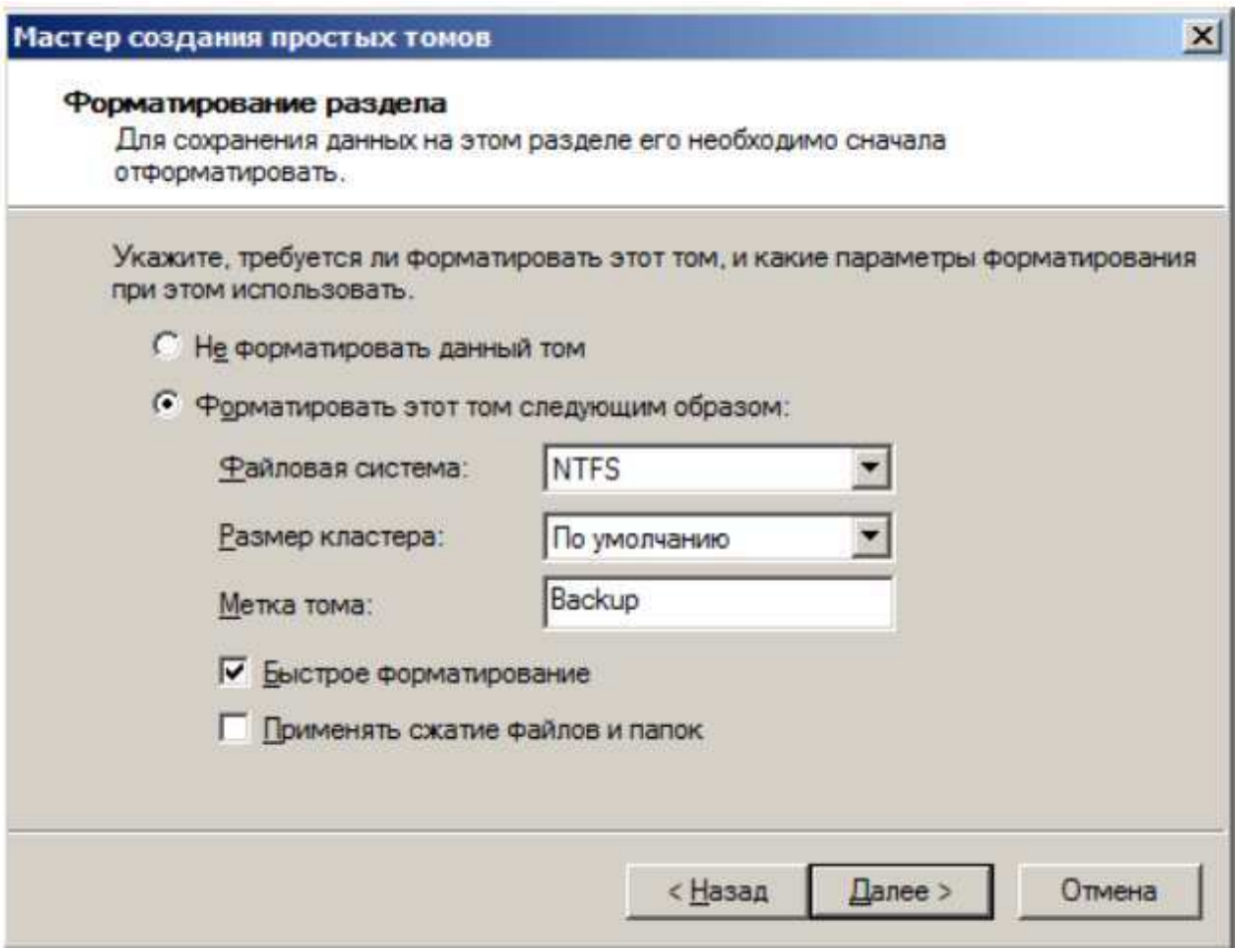


Размер выбрать ~ 10 Гб



Из получившейся не распределенной области создать новый том.





4. Изучить возможности резервного копирования с помощью остнастки “Система архивации данных Windows Server”.
a. Изучить работу мастера расписания архивации. Для этого настроить расписание архивации. Выбрать в качестве архивируемого элемента диск “C:” содержащий ОС. Архивировать раз в день в 23.00. Выполнять архивацию на том созданный ранее в работе. b. Изучить работу мастера однократной архивации. Для этого выполнить однократную архивацию папки C:\Users
c. Изучить возможность исключения файлов из резервной копии данных на основании пути или типа файла. Для этого создать на диске C:\ папку Work. Создать внутри этой папки 2 непустых документа формата txt, rtf. Далее выполнить однократную архивацию этой папки, исключив файл rtf.
d. Изучить возможность восстановления. Для этого выполнить восстановление из однократного архива который содержит файл txt.

5. Изучить возможности резервного копирование с помощью wbadmin
a. Создать папку на диске C:\Files01. Внутри этой папки

создать два непустых текстовых файла формата txt.
Создать резервную копию этой папки с помощью утилиты командной строки wbadmin. Резервная копия должна находится на диске созданном ранее в работе.

Часть 2. Cobian Backup
Часть 3. Ascomp Backup Maker

Лабораторная работа №24
Создание точек восстановления Windows в ручном и автоматических режимах. Восстановление Windows. Клонирование и восстановление ОС на примере DiskImage, HDClone, ODIN

Задание:

Часть 1. Создание точек восстановления Windows в ручном и автоматических режимах. Восстановление Windows

1. Установить Windows XP.
2. Создать точку восстановления.
3. Выяснить когда точки восстановления создаются в автоматическом режиме. Выполнить действие которое приведет к созданию автоматической точки восстановления.
4. Выполнить восстановление системы с последней точки восстановления.

Часть 2. Клонирование и восстановление ОС на примере DiskImage, HDClone, ODIN

1. Изучить работу с программой DiskImage
2. Изучить работу с программой HDClone
3. Изучить работу с программой ODIN

Лабораторная работа №25
Установка обновлений ПО и ОС с сайта производителя, автоматизация обновления, создание сервера обновлений.

Задание:

1. Создать виртуальную машину MicrisoftWindowsserver 2008
2. Вставить скриншоты всех промежуточных окон
3. Установить и настроить IIS для установки WSUS. Отразить список дополнительных ролей, возможностей, компонентов, дополнительных программ.
4. Установить и настроить WSUS.
    1. Описать варианты установки WSUS. Установить одиночный WSUS.
    2. По какому порту происходит обращение к WSUS при смене порта 80 IIS, который устанавливается по умолчанию?
    3. Какая база данных используется при установке?
    4. Установить, что обновляются только продукты на русском языке и относящиеся к семейству Office 365 (принтскрин)
    5. Установить, что синхронизация производится вручную

5. Удалить виртуальную машину MicrisoftWindowsserver 2008 32 и сопутствующие файлы.

Лабораторная работа №26
Изучение журналов и оповещений Windows и Unix, настройка службы аудита в Windows и Unix

Цель работы:ознакомление с журналами и оповещениями в операционных системах Windows, Unix. Изучение видов и назначений журналов. Изучение типов событий. Изучение служб аудита. Изучение средств для просмотра событий.
Компьютерная программа: VirtualBox, дистрибутив Windows Server 2008 R2, дистрибутив Ubuntu (версия Server или Desktop)

Порядок выполнения

Часть 1. Журналы и оповещения в Windows

Раздел про журналы и события

1. Открыть оснастку **Службы.** Найти службу Журнал событий Windows (Windows Event Log). Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.
2. Найти службу Журналы и оповещения производительности. Выписать в отчет следующие поля: описание, состояние, тип запуска, вход от имени.
3. Открыть оснастку Просмотр событий. Изучить, что отображается в окне Сводка административных событий. Изучить, что отображается в окне Сводка журнала.
4. Просмотреть все ошибки и предупреждения – для этого развернуть узел **Настраиваемые представления** и выделить **События управления**. В отчет для первых пяти событий, записать: уровень, источник, код события.
5. Создать настраиваемое представление. Отобразить все ошибки и предупреждения за последние 30 дней, для всех журналов, всех источников, всех кодов событий, всех пользователей и всех компьютеров.
6. Сохранить все события в настраиваемом представлении в новый журнал.
7. Удалите настраиваемое представление.
8. Открыть сохраненный журнал.
9. Настроить максимальный размер журнала **Установка** – 2048 КБ. Настроить **поведение при достижении максимального размера** – Архивировать журнал при заполнении; не перезаписывать события.
10. Очистить журнал **Установка,** не сохраняя содержимое.
11. Заархивировать содержимое журнала **Система.** Выбрать формат .evtx.

Раздел про оповещения

12. Открыть оснастку **Системный монитор**.
13. Прочитать содержимое окна Знакомство с монитором производительности
14. Изучить содержимое окна Сводные сведения о системе
15. Открыть Системный монитор. Добавить счетчики для памяти и для процессора. Сохранить как группу сборщиков данных.
16. Создать оповещение счетчиков производительности для счетчика: Процессор/ % загруженности процессора. Оповещение при: выше, порог: 90. Развернуть получившийся узел новой группы сборщиков данных. Открыть свойства

оповещения. Настроить **интервал выборки:** 30 сек. Настроить **действие оповещения**: Сделать запись в журнале событий приложений и **запустить группу сборщиков данных**: выбрать группу созданную ранее для памяти и процессора.

Часть 2. Журналы и оповещения в Unix

1. Запустить утилиту top и найти rsyslogd. Выписать в отчет – пользователя запустившего процесс, PID.
2. Перейти в каталог с журналам **/var/log**.
3. Вывести список всех журнальных файлов.
4. Определить назначение журналов – auth.log, boot.log, dpkg.log, kern.log, syslog.
5. Изучить содержимое файла **/etc/rsyslog.conf**
6. Изучить содержимое файла **/etc/rsyslog.d/50-default.conf**. Сделать вывод как этот файл связан с файлом /**etc/rsyslog.conf**
7. **(*** Необязательное задание) Добавить в файл /etc/rsyslog.d/50-default.conf правило для фиксации события **local5.warning** в журнал **mylog.log**. Перезапустить службу rsyslogd. С помощью команды logger добавить событие в созданный журнал – **logger –plocal5.warning "testmessage"**. Проверить наличие события в журнале.

Часть 3. Аудит в Windows

1. Настроить политику аудита: Конфигурация компьютера – Конфигурация Windows - Параметры безопасности - Локальные политики - Политика аудита.
2. Включить Аудит входа в систему, Аудит доступа к объектам.
3. Создать папку C:/Files. Настроить аудит для папки. Создавать и удалять файлы и папки в C:/Files
4. Найти в оснастке Просмотр событий – события входа/выхода пользователя в систему; события создания/удаления файлов и папок (например: Выполнение попытки получения доступа к объекту, где операция доступа: DELETE). Зафиксировать события в отчете.

Часть 4. Аудит в Unix

1. Установить auditd.
2. Найти процесс auditd.
3. Посмотреть список правил аудита **sudoauditctl –l**
4. Посмотреть файл конфигурации /etc/audit/audit.conf
5. Создать каталог /home/имя-вашего-домашнего-каталога/secret
6. Создать правило для аудита доступа к каталогу /home/имя-вашего-домашнего-каталога/secret.
7. Перезапустить auditd.
8. Открыть каталог **secret**. Создать в нем текстовый файл.

9. Выполнить aureport. Разобрать вывод.
10. Выполнить aureport –f. Разобрать вывод.
11. Найти событие в журнале аудита.

Контрольные вопросы

Про Windows:

1. Какие уровни событий бывают?
2. В какой журнал пишутся события аудита?
3. В какой консоли можно смотреть журналы событий?

Про Unix:

1. В каком каталоге находятся журнальные файлы?
2. Что такое Syslog?
3. Как работает syslogd?
4. Назовите уровни важности сообщений Syslog?
5. Какие способы обработки сообщения Syslog вы знаете?
6. Какие события можно протоколировать с помощью аудита?

Лабораторная работа №27
Управление сетями на основе протокола SNMP.

Цель: Изучить процесс управлениями сетями на основе протокола SNMP, изучить протокол SNMP.

Ход работы:

Часть 1. Изучение теоретического материала.

1. Ознакомиться с теоретическим материалом.

Часть 2. Установка и настройка программных средств

1. Установить в VirtualBox (на рабочих столах) - ОС Ubuntu. (Дистрибутив в файлообменнике \\10.7.3.3\Shared\soft)
2. Запустить Ubuntu.
3. Установить snmp пакет, выполнив в gnome-terminal: sudo apt-get install snmp
4. Выполнить: sudo apt-get install snmp-mibs-dowloader
5. Выполнить:

Часть 3. Изучение утилит snmp (Описание утилит приведено в теоретических материалах).

1. Изучить работу утилит snmp:
2. Выполнить: snmptranslate .1.3.6.1.2.1.1.3.0
3. Выполнить: snmptranslate 1.3.6.1.2.1.5.1
4. Выполнить: snmpget -c demopublic -v 2c test.net-snmp.org system.sysUpTime.0
5. Выполнить: snmpgetnext -v 2c -c demopublic test.net-snmp.org system.sysUpTime.0
6. Выполнить: snmpwalk -v 2c -c demopublic test.net-snmp.orgsystem
7. Выполнить: snmptable -v 2c -c demopublic test.net-snmp.org sysORTable
8. Определить результаты работы утилит.
9. Знать ответы на контрольные вопросы (находятся в конце документа).

Часть 4. Изучение SNMP в Cisco Packet Tracer

1. Добавить роутер (Router-PT) и ПК.
2. Настроить интерфейсы:
3. Настроить роутер:

```
Router# configure terminal
Router(config)# snmp-server community [name1] ro
Router(config)# snmp-server community [name2] rw
Router(config)# ctrl+z
Router# write
```

4. Настроить ПК:

Выделите ПК, откройте MIB-browser, во вкладке введите следующиезначения:

```
Address          [IP address of router's connected interface]
Port             161
```

Read Community [name1]
Write community [name2]
SNMP Version v 35. В MIB-Browser в ПК для роутера:
- изменить имя роутера: MyRouter
- получить список интерфейсов роутера
- включить интерфейс FastEthernet1/0

Контрольные вопросы:
1. Для чего используется SNMP?
2. Что такое MIB?
3. Назначение утилиты snmptranslate?
4. Назначение утилиты snmpget?

Лабораторная работа №28
Анализ сетевого трафика средствами Сетевого монитора

Цели работы:научиться устанавливать MicrosoftNetworkMonitor, изучить назначение основных элементов программы, производить анализ трафика.

Оборудование: ПК, ЛВС, MicrosoftNetworkMonitor 3.4.

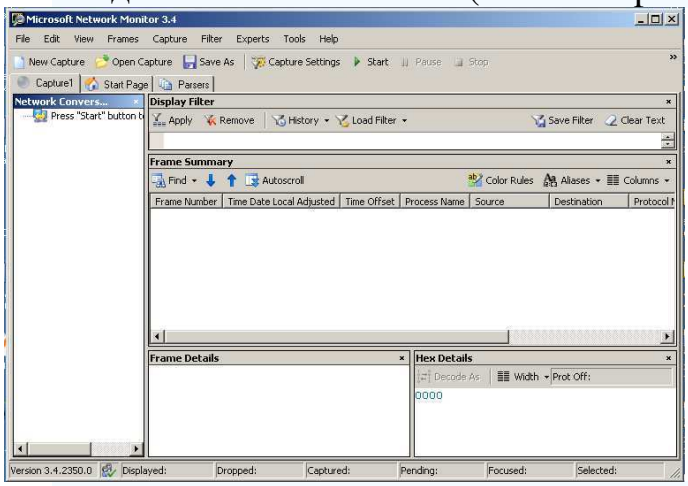
Теоретическая часть

Сетевой монитор (**Network Monitor**) представляет собой анализатор пакетов и инструмент захвата фреймов, помогающий в определении таких инкапсуляций, и является крайне важным инструментом для любого сетевого администратора и администратора безопасности.

Одной из лучших функций продукта является возможность отслеживания трафика и его привязки к работающему процессу, в результате чего администратор может быстро определить приложение, которое разговаривает с машиной, а также тип передаваемого трафика, без необходимости обработки больших объемов трафика.

Ход работы

1. Скачайте MicrosoftNetworkMonitor 3.4. с сайта производителя.
2. Установите MicrosoftNetworkMonitor 3.4. в соответствии с инструкцией производителя.
3. Создайтеновыйзахватчик (Recent Captures – New capture Tab).



4. Для начала анализа трафика, нажмите кнопку Start.
5. Просмотрите какую информацию вы получите в результате анализа
6. Вывод

Лабораторная работа №29
Установка и использование программы Wireshark.

Цель: научиться устанавливать и использовать программу Wireshark.

Ход работы:

Часть 1. Изучить теоретический материал.

Часть 2. Использование программы Wireshark.

Изучить принципы работы и проанализировать пакеты.

Схема анализа:
Начать захват. Эмулировать сетевую активность, чтобы получить пакеты нужного типа (веб-браузер, команды). Остановить захват. Проанализировать результаты.
* В скобках указан утилиты командной строки, которые надо использовать при эмуляции сетевой активности, чтобы получить пакеты нужного типа.

-ARP (arp)
-IP
-TCP
-UDP
-DNS (nslookup ya.ru)
-ICMP (ping)
-HTTP

Лабораторная работа №30
Мониторинг сетевой активности и производительности.

Цель: Изучить процесс мониторинга сетевой активности и производительности на примере программы Nagios.

Ход работы:

Часть 1. Изучить теоретический материал

Часть 2. Установка Nagios. Выполнить в виртуальной машине (для ОС Ubuntu):

Зайти в консоль с правами root:
#sudo su

Ввести свой пароль. Скачать и установить необходимые пакеты:
#apt-get install apache2 php5 nagios3

Во время установки “postfix configuration” - выбрать"без настройки" и ввести пароль для учетной записи nagiosadmin: 123

После окончания установки зайти на веб-интерфейс вашего Nagios. Для примера IP 192.168.0.1:
http://192.168.0.1/nagios3/

Часть 3. Настройка пользователей Nagios.

Все конфигурационные файлы лежат в /etc/nagios3/. Главный конфигурационный файл nagios.cfg в нём подключаются все остальные конфигурационные файлы и задаются настройки самого nagios.
Файл cgi.cfg - в нём выставляются все настройки cgi скриптов, так же в нём выставляются права на доступ к сайту с графическим интерфейсом.

Напротив нижеследующих переменных убираем пользователя nagiosadmin и прописываем ваш логин (myuser в примере). Если админов несколько, то пишем через запятую.

default_user_name=myuser
authorized_for_system_information=myuser

```
authorized_for_configuration_information=myuser
authorized_for_system_commands=myuser
authorized_for_all_services=myuser
authorized_for_all_hosts=myuser
authorized_for_all_services=myuser
authorized_for_all_hosts=myuser
authorized_for_all_service_commands=myuser
authorized_for_all_host_commands=myuser
```

Где myuser - это ваш логин. Теперь нужно создать файл с пользователями и паролем, для этого перейдите в каталог /etc/nagios3 выполнить команды:

```
#cd  /etc/nagios3/
#htpasswd -c htpasswd.users myuser
```
и ввести пароль для пользователя myuser

Теперь чтобы изменения вступило в силу перезагрузите nagios
```
# /etc/init.d/nagios3 restart
```

Так же можно проверять весь конфиг nagios перед перезагрузкой.
```
#nagios3 -v  /etc/nagios3/nagios.cfg
```

Он проверит файл nagios.cfg и все файлы которые подключаются в нём и если найдёт ошибки напишет подробную информацию, я советую делать такую проверку после каждого изменения в конфигурационных файлах.

После окончания зайти в браузере 127.0.0.1/nagios - под новым пользователем.

Часть 4. Добавление хостов.

Создаём в каталоге /etc/nagios3/conf.d файл my-hosts.cfg и записываем в него хосты пяти одногруппников.

```
#  определение хоста товарища
define host {
        host_name   hostname                #Имя хоста
alias       name comp               #описание
```

```
        address     192.168.140.3           #ip адрес
        use         generic-host
}
 … # далее еще четыре записи хостов товарищей в таком формате
```

Так как этот файл находится в каталоге /etc/nagios3/conf.d отдельно подключать его в файле /etc/nagios3/nagios.cfg не надо, поскольку в нём уже по умолчанию подключаются все файлы из Директории /etc/nagios3/conf.d

Объединим эти хосты в группу. Запишем в конфигурационный файл групп /etc/nagios3/conf.d/hostgroups_nagios2.cfg такой текст

```
# Определяемгруппу
define hostgroup {
        hostgroup_name  my-friends                              #имягруппы
alias           my-friends comps                        # описание
                members         hostname, hostname2, hostname3...       #члены группы
}
```

Теперь надо настроить службу которая будет проверять эту группу хостов. Дописываем в файл /etc/nagios3/conf.d/services_nagios2.cfg или создаём свой файл с таким конфигом.

```
# проверяем включены ли компьютеры товарищей
define service {
        hostgroup_name      my-friends      #имя группы для проверки
        service_description     PING
        check_command       check_ping!100.0,20%!500.0,60%#команда проверки
        use             generic-service
}
```

Часть 5. Настроить уведомления по email.

Для рассылки уведомлений создайте контакт в файле

/etc/nagios3/conf.d/contacts_nagios2.cfg Например такой.

```
define contact{
        contact_name                    myuser      #имя
alias                           myuser
        service_notification_period     24x7          #период уведомлений о сервисах
        host_notification_period        24x7          #период уведомлений о хостах
        service_notification_options    w,u,c,r       #о чём уведомлять уведомлений
        host_notification_options       d             #уведомлять о том что хост down
        service_notification_commands   notify-service-by-email  #как уведомлять
        host_notification_commands      notify-host-by-email #как уведомлять
        email                           myemail@someserver.ru  # mail ващ почтовый ящик
}
```

Временные периоды задаются в файле /etc/nagios3/conf.d/contacts_nagios2.cfg там уже есть несколько уже заданных по умолчанию периода, по их аналогу Вы легко зададите свои.

Часть 6. Настроить Nagios для мониторинга Windows-хостов.
Добавить в файлы настроек - настройки для Windows-хоста.

Пример файла настроек для Windows хоста:

```
# Описание узла (IP адрес, имя)
define host{
use  generic-host
host_name server01
alias Windows Server
address 192.168.1.20 #тутпроизвольный IP адрес
}
```

Настройка сервисов:

```
# Описание контролируемых сервисов
define service{
use generic-service
host_name server01
```

```
service_description NSClient++ Version
check_command check_nt!CLIENTVERSION # Командадляпроверки
}

# Расход оперативной памяти
define service{
use generic-service
host_name server01
service_description Memory Usage
check_command check_nt!MEMUSE!-w 80 -c 90
}
# Чтобы добавить контроль конкретного сервиса (например Explorer), используем такую конструкцию:
define service{
use generic-service
host_name server01
service_description Explorer
check_command check_nt!PROCSTATE!-d SHOWALL -l Explorer.exe
}
```

Для того чтобы начать мониторинг Windows-хоста на нем должна быть установлена специальная программа-клиент NSClient++.
У нас нет возможности одновременно запустить Ubuntu и Windows Server 2003 (на сервере virtual) поэтому - клиент устанавливать не надо. Но “как это сделать” - знать надо - поэтому читаем ниже.

На странице для закачки www.sf.net/projects/nscplus можно загрузить zip-архив или установочный файл. Обратите внимание, что для 32- и 64-битных систем берутся разные файлы. Установка msi-файла стандартна – в случае zip-архива его нужно распаковать, а затем, перейдя в этот каталог, ввести в окне терминала две команды:

```
> nsclient++ /install
> nsclient++ SysTray
```

После этого в консоли «Службы» появится новый сервис. Вызываем окно свойств, переходим на вкладку «Вход в систему» и взводим флажок «Разрешить взаимодействие с рабочим столом». Запустить ее можно, введя в терминале:

> nsclient++ /start

Перед запуском изменить параметры в конфигурационном файле NSC.ini, который находится в подкаталоге, где установлен NSClient++. Несмотря на то, что параметров внутри много, зачастую достаточно просто снять комментарии.

Часть 7. Настроить мониторинг web-сервера.
-Создать новый хост

```
define host {
host_name   yaru #выберите произвольный сайт
 alias          yaru#
 address       ya.ru
 use                  generic-host
 }
```

Далее создайте группу, куда включите этот хост - например web-sites.

```
#web sites
define hostgroup {
        hostgroup_name web-sites
                alias web servers
                members yaru
}
```

Далее создайте сервис куда включите группу созданную ранее.

```
#web sites
define service {
        hostgroup_name                  web-sites
        service_description             HTTP
        check_command                   check_http
        use                             generic-service
        notification_interval           0 ; set > 0 if you want to be renotified
}
```

Часть 8. Заменить логотипы отображаемых элементов на карте Nagios.
Логотипы находятся в /usr/share/nagios/htdocs/images/logos, при изменении логотипа достаточно лишь указать новое картинки, находящейся по указанному пути.
Редактируем файл :
nano /etc/nagios3/conf.d/extinfo_nagios2.cfg

```
define hostextinfo{
      hostgroup_name   my-group #тутимявашейгруппы
      notes            my-servers #описание
```

```
    icon_image      base/name_of_image.png #картинка
    icon_image_alt   my-servers
    vrml_image      name_of_image.png
    statusmap_image  base/name_of_image.gd2
    }
```

Картинкиизпапки /usr/share/nagios/htdocs/images/logos выбратьсамостоятельно.

Часть 9. Обновить схему.
- Добавить к существующим хостам: сервер 10.7.3.3, сервер 10.7.3.1
- Добавить группу серверы - добавить туда серверы.
- Добавить сервис PING - для группы серверов.
- Назначить группе правильную картинку (чтобы было видно что это сервер).
- Добавить сайты pkjt.karelia.ru, google.com в группу web-сайтов (сервис check_http).

Теоретический материал

Настройки сети в VirtualBox во время выполнения лабораторной работы

Трансляция сетевых адресов (NAT)

Протокол NAT позволяет гостевой операционной системе выходить в Интернет, используя при этом частный IP, который не доступен со стороны внешней сети или же для всех машин локальной физической сети. Такая сетевая настройка позволяет посещать web-страницы, скачивать файлы, просматривать электронную почту. И все это, используя гостевую операционную систему. Однако извне невозможно напрямую соединиться с такой системой, если она использует NAT.

Принцип трансляции сетевых адресов заключается в следующем. Когда гостевая ОС отправляет пакеты на конкретный адрес удаленной машины в сети, сервис NAT, работающий под VirtualBox, перехватывает эти пакеты, извлекает из них сегменты, содержащие в себе адрес пункта отправки (IP-адрес гостевой операционной системы) и производит их замену на IP-адрес машины-хоста. Затем заново упаковывает их и отправляет по указанному адресу.

Например, в вашей домашней локальной сети хост и другие физические сетевые устройства имеют адреса в диапазоне, начинающемся с 192.168.x.x. В VirtualBox адаптеры, работающие по протоколу NAT, имеют IP-адреса в диапазоне, начинающемся с 10.0.2.1 и заканчивающемся 10.0.2.24. Такой диапазон называется под-сетью. Как правило, этот диапазон не используется для присвоения адресов устройствам в основной сети, поэтому такая система недоступна извне, со стороны хоста. Гостевая ОС может выполнять обновление программного обеспечения и web-серфинг, но остается

невидимой для остальных "участников".
В руководстве VirtualBox этот момент описан более подробно:
"В режиме NAT гостевому сетевому интерфейсу присваивается по умолчанию IPv4 адрес из диапазона 10.0.x.0/24, где x обозначает конкретный адрес NAT-интерфейса, определяемый по формуле +2. Таким образом, x будет равен 2, если имеется только один активный NAT-интерфейс. В этом случае, гостевая операционная система получает IP-адрес 10.0.2.15, сетевому шлюзу назначается адрес 10.0.2.2, серверу имен (DNS) назначается адрес 10.0.2.3." (Oracle Corporation, 2012, Глава 9).
Протокол NAT полезен в том случае, когда нет разницы в том, какие IP-адреса будут использовать гостевые ОС на виртуальной машине, поскольку все они будут уникальными. Однако, если потребуется настроить перенаправление сетевого трафика, или же расширить функциональность гостевой ОС, развернув на ней web-сервер (к примеру), то необходимы дополнительные настройки. В режиме NAT также недоступны такие возможности, как предоставление общего доступа к папкам и файлам.

Сетевой мост (Bridged)
В соединении типа "Сетевой мост" виртуальная машина работает также, как и все остальные компьютеры в сети. В этом случае адаптер выступает в роли моста между виртуальной и физической сетями. Со стороны внешней сети имеется возможность напрямую соединяться с гостевой операционной системой.
Адаптер в режиме "Сетевой мост" подключается, минуя хост, к устройству, которое распределяет IP-адреса внутри локальной сети для всех физических сетевых карт. VirtualBox соединяется с одной из установленных сетевых карт и передает пакеты через нее напрямую; получается работа моста, по которому передаются данные. Как правило, адаптер в модели "Сетевой мост" получает стандартный адрес из диапазона 192.168.x.x от роутера. Поэтому виртуальная машина в сети выглядит так, как будто это обычное физическое устройство, неотличимое от остальных.
На хосте могут быть активными одновременно несколько сетевых устройств; например, на моем ноутбуке имеется проводное подключение (называемое eth0) и беспроводное подключение (называемое wlan0). Поле "Имя" позволяет выбрать, какой из сетевых интерфейсов вы бы хотели использовать в качестве моста на VirtualBox.

Протокол NAT полезен, потому что он защищает гостевые операционные системы со стороны Интернет. Но для того, чтобы получить доступ к ним извне (а на некоторых ОС у меня имеются установленные web-сервера), потребуется дополнительная настройка для перенаправления трафика. Тип подключения "Сетевой мост" позволяет получить доступ к ним, но системы в этом случае становятся незащищенными.
Если ваше сетевое устройство доступа (это может быть маршрутизатор, сетевой коммутатор или же настройки, предоставленные Интернет-провайдером) позволяет

предоставлять только один IP-адрес для сетевого интерфейса, возможно, вам не удастся настроить "Сетевой мост".

За что админы любят Nagios

Nagios производит мониторинг работы большинства сетевых сервисов: SMTP, POP3, IMAP, SSH, Telnet, FTP, HTTP, DNS и многих других. Также с его помощью можно отслеживать использование ресурсов серверов: загруженность процессора, расходование оперативной памяти, дискового пространства и т.д. – причем, не только в Unix, но и в других ОС. Например, мониторинг работы серверов под управлением Windows обеспечивается модулем NRPE_NT.

Возможен удаленный мониторинг через шифрованные SSH- или SSL-туннели. Простая архитектура модулей расширений позволяет создавать свои способы проверки служб и обработчики событий (к примеру, перезапуск зависшего сервиса). Концепция «родительских» узлов дает возможность определить иерархию и зависимости между хостами. Таким образом можно отличать действительно неработающие узлы от тех, которые недоступны системе мониторинга из-за неполадок на промежуточных пунктах. Nagios ценят за умение строить карты сетевой инфраструктуры и графики различных параметров наблюдаемых систем.

Проект возник в 2002 году, хотя первое время он был известен как NetSaint. Его лидером является программист Этан Галстад. Само слово Nagios, по информации на сайте www.nagios.org, – это рекурсивный акроним, который расшифровывается, как Nagios Ain't Gonna Insist On Sainthood («Nagios не собирается настаивать на святости») – намек на предыдущее название проекта. Функциональность расширяется за счет плагинов и аддонов, большая часть из которых доступна на странице закачки.

Сейчас предлагается две ветки продукта: 2.x и 3.x. В последней не только исправлены найденные ранее ошибки, добавлены новые макросы и многое другое, но, что важно, пересмотрен алгоритм сканирования, с целью устранить один из главных недостатков этой системы – медлительность при проверке больших сетей. В 2.x все тесты проходят практически последовательно, а в новой редакции задачи выполняются параллельно. Хотя вторая версия еще развивается, очевидно, что в будущем все силы будут брошены на третью ветку. Поэтому, хотя отличия в настройках незначительны, дальше речь пойдет именно о ней.

Конфигурационные файлы Nagios

Как отмечалось выше, после установки Nagios появится несколько конфигурационных файлов. Основной конфиг, содержащий большое количество директив, которые демон

считывает при запуске, называется nagios.cfg. Этот файл ссылается еще на два типа файлов. В файлах ресурсов содержатся пользовательские макросы, в том числе и пароли для доступа к объектам. Эту информацию специально разместили отдельно, чтобы не было возможности получить к ней доступ из CGI. В целях безопасности на такие файлы устанавливаются права 600 или 660. По умолчанию файл ресурсов один – resource.cfg.

Использовав директиву resource_file в nagios.cfg, можно добавить любое их количество. Объекты, то есть все элементы, участвующие в мониторинге и оповещении (узлы, сервисы, контакты, команды и т.д.), описываются файлами определения объектов (Object Definition Files). За счет cfg_file можно прописать несколько таких файлов, но для удобства вместо отдельных файлов используют директиву cfg_dir. С ее помощью можно указать Nagios на каталог, где он будет искать файлы с описаниями объектов.И, наконец, файл cgi.cfg содержит настройки CGI.
Параметров в nagios.cfg и cgi.cfg довольно много, но часто их назначение – очевидно. Полное описание всех параметров конфигурационных файлов можно найти в документации Nagios (nagios.sf.net/docs/3_0). Файл ресурсов очень прост. Наибольший интерес представляют объектные файлы. Чтобы пример сделать интереснее, настроим мониторинг удаленного сервера, работающего под управлением Windows.