

Министерство общего и профессионального образования Ростовской области
НОВОШАХТИНСКИЙ ТЕХНИКУМ ПРОМЫШЛЕННЫХ ТЕХНОЛОГИЙ –
филиал государственного бюджетного профессионального образовательного
учреждения Ростовской области
«ШАХТИНСКИЙ РЕГИОНАЛЬНЫЙ КОЛЛЕДЖ
ТОПЛИВА И ЭНЕРГЕТИКИ
им. ак Степанова П.И.»

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ
ПО ПРОВЕДЕНИЮ ПРАКТИЧЕСКИХ ЗАНЯТИЙ**
**по дисциплине МДК 03.01 Техническое обслуживание и ремонт компьютерных
систем и комплексов**
для обучающихся очного отделения
09.02.01 Компьютерные системы и комплексы (базовая подготовка СПО)

Практическое занятие 1,2

Методика поиска неисправностей элементов БП ПК

Тема: Методика поиска неисправностей элементов БП ПК

Цель: Изучить методику и порядок работы при поиске неисправностей элементов БП ПК.

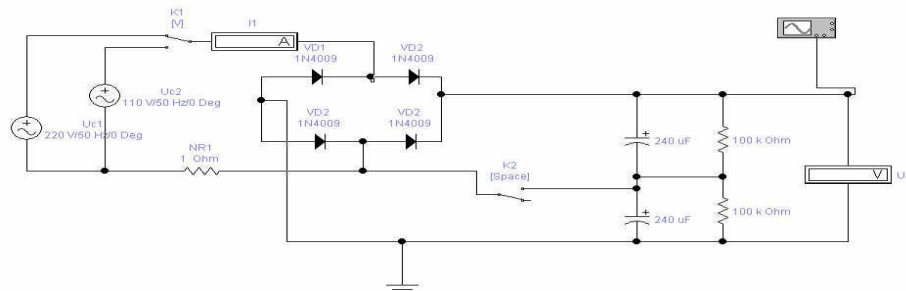
Оснащение: ПК, программа EWB и программные модели сетевого выпрямителя БП ПК - CetV.EWB, программная модель схемы выработки сигнала PG (два варианта) - pg.ewb и pg1.ewb.

Порядок выполнения занятия

Теоретические сведения

Методика проверки работы сетевого выпрямителя и фильтра.

Ознакомится с признаками исправной работы сетевого выпрямителя и фильтра, для этого загрузить модель выпрямителя - CetV.EWB. Проверить исходной состояние переключателей K1-вверх, K2-вниз, что соответствует работе БП от источника ~220В.



Ознакомится с критериями исправной работы сетевого выпрямителя при работе от источника ~220В, записав значение величины выходного напряжения U1, тока потребляемого выпрямителем II и величины пульсаций выпрямленного напряжения (измерив с помощью осциллографа).

Изменив положение переключателей K1- вниз, K2- вверх, ознакомится с критериями исправной работы сетевого выпрямителя при работе от источника ~127В, записав значение величины выходного напряжения U1, тока потребляемого выпрямителем II и величины пульсаций выпрямленного напряжения (измерив с помощью осциллографа).

Изменить положение K1- вверх, измерить значение U1. Сделать вывод к чему приведут такие действия на реальном БП. **Восстановить исходное состояние переключателей K1и K2.**

Ознакомится с основными признаками неисправности сетевого выпрямителя с неисправными диодами VD1-VD4 .

Выполнив двойной щелчок ЛКМ по диоду VD1 в открывшемся окне, на закладке «Fault», ввести неисправность Shot (пробой). Включить процесс моделирования неисправного выпрямителя и ознакомится с признаком неисправной работы сетевого выпрямителя, записав значение величины выходного напряжения U1, тока потребляемого выпрямителем II и величины пульсаций выпрямленного напряжения (с помощью осциллографа).

Последователь вводя неисправности диодов VD2-VD4 ознакомится с признаками неисправности сетевого выпрямителя. Результаты измерений занести в таблицу 1.

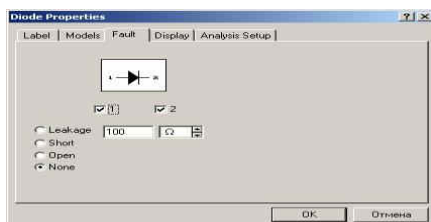


Таблица 1

Неисправные элементы	Измеренные значения		
	Напряжение U1, В	Потребляемый ток	Пульсация,

		I_1 , А	выпрямленного напряжения, мВ
VD1			
VD1, VD2			
VD1, VD2, VD3			
VD1, VD2, VD3, VD4			

Восстановить исправность диодов VD1-VD4, введя на закладке «Fault» значение None (нет). Ознакомится с основными признаками неисправности конденсаторов фильтра C1, C2. Выполнив двойной щелчок ЛКМ по конденсаторов фильтра C1 в открывшемся окне, на закладке «Fault», ввести неисправность Shot (пробой) затем Open (обрыв). Последователь вводя неисправности конденсаторов фильтра C1, C2 ознакомится с признаками неисправности сетевого выпрямителя. Результаты измерений занести в таблицу 1.

Таблица 2

Неисправные элементы	Измеренные значения		
	Напряжение U_1 , В	Потребляемый ток I_1 , А	Пульсация, выпрямленного напряжения, мВ
(пробой)			
(обрыв)			
C1,C2(пробой)			
C1,C2(обрыв)			

Контрольные вопросы.

Какие методы ремонта применяются при ремонте БП?

Какие основные неисправности БП существуют.

Какова последовательность действий при ремонте сетевого выпрямителя и фильтра?

Какие основные признаки исправной работы сетевого выпрямителя и фильтра БП?

Какие основные признаки исправной работы схемы выработки сигнала P G БП?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 3

Методика тестирования мс ШИМ контроллера TL494 БП ПК

Цель: Изучить методику и порядок работы при тестировании ШИМ контроллера TL494 БП ПК.

Оснащение: ПК, программа EWB и программные модель ШИМ контроллера- tl494.ewb, программная модель схемы инвертора -pg.ewb и pg1.ewb.

Порядок выполнения работы

Теоретические сведения

Типовые неисправности БП ПК ОДНОЙ ИЗ САМЫХ ХАРАКТЕРНЫХ НЕИСПРАВНОСТЕЙ является "пробой" диодов выпрямительного моста сетевого выпрямителя или мощных ключевых транзисторов инвертора.

При КЗ в первичной цепи ИБП выгорает (со взрывом) токоограничивающий терморезистор с отрицательным ТКС.

ВТОРОЙ ХАРАКТЕРНОЙ НЕИСПРАВНОСТЬЮ ИБП является выход из строя управляющей микросхемы ШИМ контроллера типа TL494. Исправность микросхемы можно установить, оценивая работу отдельных ее функциональных узлов (без выпаивания из схемы ИБП).

ТРЕТЬЕЙ ХАРАКТЕРНОЙ НЕИСПРАВНОСТЬЮ является выход из строя выпрямительных диодов во вторичных цепях ИБП. Правильность работы схемы выработки сигнала PG. Работоспособность цепей обратной связи и защиты от перенапряжений.

Методика проверки ШИМ контроллера TL494:

Операция 1. Проверка исправности генератора DA6 и опорного источника DA5

Не включая ИБП в сеть, подать на вывод 12 управляющей микросхемы питающее напряжение 10-15В от отдельного источника

Исправность генератора DA6 оценивается по наличию пилообразного напряжения амплитудой 3.2В на выводе 5 микросхемы (при условии исправности частото задающих конденсатора и резистора, подключенных к выводам 5 и 6 микросхемы, соответственно).

Исправность опорного источника DA5 оценивается по наличию на выводе 14 микросхемы постоянного напряжения +5В, которое не должно изменяться при изменении питающего напряжения на выводе 12 от +7В до +40В.

Операция 2. Проверка исправности цифрового тракта.

Не включая ИБП в сеть, подать на вывод 12 управляющей микросхемы питающее напряжение 10-15В от отдельного источника. Исправность цифрового тракта оценивается по наличию на выводах 8 и 11 микросхемы (в случае включения выходных транзисторов микросхемы по схеме с ОЭ) или на выводах 9 и 10 (в случае их включения по схеме с ОК) прямоугольных последовательностей импульсов в момент подачи питания.

Проверить наличие фазового сдвига между последовательностями выходных импульсов, который должен составлять половину периода. **Операция 3** Проверка исправности компаратора "мертвой зоны" DA1.

Не включая ИБП в сеть, подать на вывод 12 управляющей микросхемы питающее напряжение 10-15В от отдельного источника. Убедиться в исчезновении выходных импульсов на выводах 8 и 11 при замыкании вывода 14 микросхемы с выводом 4. **Операция 4.** Проверка исправности компаратора ШИМ DA2.

Не включая БП в сеть, подать на вывод 12 управляющей микросхемы питающее напряжение 10-15В от отдельного источника. Убедиться в исчезновении выходных импульсов на выводах 8 и 11 при замыкании вывода 14 микросхемы с выводом 3. **Операция 5** Проверка исправности усилителя ошибки DA3.

Не включая БП в сеть, подать на вывод 12 управляющей микросхемы питающее напряжение 10-15В от отдельного источника. Проконтролировать уровень напряжения на выводе 3, которое должно отличаться от нуля. Изменяя напряжение на выводе 1, подаваемое от

отдельного источника питания, в пределах от 0.3В до 6В: проконтролировать изменение напряжения на выводе 3 микросхемы.

Порядок выполнения работы:

Порядок выполнения работы:

Методика проверки работоспособности мс ШИМ контроллера TL494.

Результаты тестирования представить в виде таблицы 1. Таблица 1.

/п	Наименование пункта проверки	Значения проверяемого параметра	
		Должно быть	Полученное значение

Ознакомится с признаками исправной работы ШИМ контроллера, для этого загрузить модель ШИМ контроллера- **tl494.ewb**. Проверить исходной состояние переключателей К1 К2, К3 -вверх, что соответствует работе в БП. Источник E1 имитирует напряжение с выхода БП.

Рис 1. Исследуемая модель мс TL494

Выполнить проверку исправности генератора DA6 и опорного источника DA5. Для этого: подключив вольтметр V2 к 14 выводу микросхемы проверить наличие постоянного напряжения не менее +5В, которое не должно изменяться при изменении питающего напряжения на выводе 12 E2 от +7В до +40В. Для изменения напряжения выполнить двойной щелчок правой кнопкой мыши по источнику питания. В открывшемся окне ввести требуемое значение.

подключив вход осциллографа к выводу 5 микросхемы проверить наличие пилообразного напряжения амплитудой не менее 4В (измерение выполнять с помощью осциллографа).

Выполнить проверку исправности цифрового тракта мс. Для этого: С помощью осциллографа проверить наличие на выводах 8 и 11 микросхемы прямоугольных последовательностей импульсов.

Изменяя (клавиши R и R+Shift) величину напряжения на выводе 1 мс проверить изменение длительности импульса при неизменном периоде их повторения (ШИМ регулирование). Выполнить измерение наибольшего и наименьшего значения длительности импульса. Зарисовать полученные осциллограммы.

Проверить отсутствие фазового сдвига между последовательностями выходных импульсов, при переключении ключа К3 в нижнее положение. Зарисовать полученные осциллограммы.
Вернуть К3 в исходное состояние.

Выполнить проверку исправности компаратора "мертвой зоны" DA1. Для этого:

С помощью осциллографа убедиться в исчезновении выходных импульсов на выводах 8 и 11 при замыкании с помощью ключа К1 вывода 14 микросхемы с выводом 4.

1.1.18. Проверка исправности компаратора ШИМ DA2. Для этого:

С помощью осциллографа убедиться в исчезновении выходных импульсов на выводах 8 и 11 при замыкании с помощью ключа К2 вывода 14 микросхемы с выводом 3.

1.1.19. Проверка исправности усилителя ошибки DA3. Для этого:

Подключив вольтметр V1, проконтролировать уровень напряжения на выводе 3, которое должно отличаться от нуля. Изменяя напряжение на выводе 1, подаваемое от отдельного источника питания (клавиши R и R+Shift), в пределах от 0.3В до 6В: проконтролировать изменение напряжения на выводе 3 микросхемы.

Контрольные вопросы.

Какие методы ремонта применяются при ремонте БП?

Какие основные неисправности БП существуют.

Какова последовательность действий при ремонте сетевого выпрямителя и фильтра?

Какие основные признаки исправной работы сетевого выпрямителя и фильтра БП?

Какие основные признаки исправной работы схемы выработки сигнала P G БП?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Практическое занятие 4,5

Методика тестирования материнской платы ПК с помощью программы Checkit

Цель: Изучить методику программного способа тестирования материнской платы и порядок работы спрограммой Checkit при выполнении тестирования.

Оснащение: ПК, программа Checkit, технологические заглушки для проверки портов ПК.

Порядок выполнения работы

Теоретические сведения

Основная и самая сложная плата ПК называется материнской (mainboard), системной платой (СП), поскольку она содержит "сердце" ПК - микропроцессор. На ней также размещены несколько сверхбольших интегральных схем (СБИС), ОЗУ, ПЗУ и ряд других микросхем, переключатели - перемишки режимов работы ПК, разъемы расширения для подключения плат адаптеров и контроллеров.

Процессор—главная деталь в системе, он подключен практически ко всем узлам платы, кроме МЮ, и то на многих старых платах сигнал вентиля GATE A20 заводится с МЮ.

ВИП1—первый вторичный источник питания, все процессоры начиная с Pentium MMX имеют двойное питание. Стабилизаторы практически всегда импульсные и для их реализации используются специальные микросхемы. Обладают большой мощностью, и выходные каскады почти всегда имеют дополнительное охлаждение.

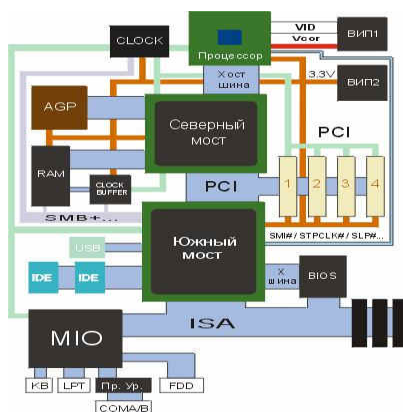
ВИП2—второй вторичный источник питания используется для питания всех устройств не питающихся от 5В. Не смотря на то, что у источника питания АТХ формата есть источник на 3.3 вольта, многие цепи питания имеют дополнительные стабилизаторы на плате.

CLOCK — опорный генератор, все устройства на материнской плате синхронизируются одним опорным генератором, система синхронизации на структурной схеме изображена достаточно условно. В общем случае в компьютере существуют следующие тактовые частоты:

• **Host Bus Clock (CLK2IN)** — это опорная частота (внешняя частота шины процессора). Именно из нее могут получаться другие частоты и именно она задается перемишками (джамперами);

CPU Clock (Core Speed) — это внутренняя частота процессора, на которой работает его вычислительное ядро. Может совпадать с Host Bus Clock или получаться из нее умножением на 1,5, 2, 2,5, 3, 4. Умножение должно быть предусмотрено в конструкции процессора.

ISA Bus Clock (ATCLK, VBUSCLK) — это тактовая частота системной шины ISA (сигнал SYSCLK). По стандарту она должна быть близка к 8 МГц, но в BIOS Setup имеется возможность выбрать ее через коэффициент деления частоты Host Bus Clock. Иногда компьютер остается работоспособным и при частоте шины ISA около 20 МГц, но обычно платы расширения ISA разрабатываются из расчета на 8 МГц, и при больших частотах они перестают работать. Не следует рассчитывать, что компьютер станет вдвое быстрее при удвоении этой частоты. Для каналов прямого доступа к памяти на системной плате используется еще один тактовый сигнал SCLK, частота которого, как правило, составляет половину от ISA Bus Clock.



PCI Bus Clock — это тактовая частота системной шины PCI, которая по стандарту должна быть 25 — 33,3 МГц. Ее обычно получают делением частоты Host Bus Clock на нужный коэффициент.

В компьютерах предусматривается возможность ее увеличения до 75 или даже 83 МГц, но из соображений надежности работы рекомендуется придерживаться стандартных значений.

VLB Bus Clock —это частота локальной шиныVLB,определяемая аналогичноPCI Bus Clock.

CLOCK BUFFER –буфер опорного генератора используется не на всех платах.В тех платах,где чипсет управляетсинхронизацией памяти, служит для буферизации сигналов синхронизации, например, используется в материнских платах на

VT82C694X.

МІО – Multi Input Output chipмикросхема системы ввода вывода.Включает в себя:

Floppy Drive Controller – контроллер накопителя на гибких дисках,

CMOS – энерго-независимая память,

RTC – Real Time Clock часы реального времени,

контроллер последовательного и паралельного интерфейсов (COMA COMB LPT), контроллер клавиатуры

система мониторинга состояния системной платы. Во многих чипсетах МІО интегрировано в южный мост частично или полностью например VT82C686B.

Пр. Ур. – преобразователь уровня, обязательно используется для реализации COM. МІО имеет 5 вольтовый интерфейс, а COM порт 12 вольтовый.

BIOS –BasicInput Output Systemосновная система ввода вывода,реализуется обычно в видеEEPROM –попросту энерго-независимая память,объем обычно колеблется от1Мбит до4Мбит(128КБайт до 1024КБайт). Служит для управления системой до загрузки операционной системы. Именно программу записанную в BIOS, машина выполняет по включении системы.

AGP –Accelerated Graphic Port–ускоренный графический порт,шина ориентированная на использование высоко производительных видеоадаптеров.Высокая скорость передачиобеспечивается конвейеризацией обращений к памяти. По спецификации в очередь может быть установлено до 256 запросов на обращение к памяти!!!

RAM –Random Access Memory–память случайного доступа,или попросту память.

PCI –Peripheral Component Interconnector–конектор для подсоединения внутренних периферийных устройств.Синхронная шина с совмещенной шиной адреса,данных и команд,позволяющая достигать скорости передачи данных до 133Мбайт/с или в PCI64 до 266Мбайт/с.

ISA –Industry Standard Architecture–индустриальный стандарт архитектуры,на сегодня устаревшая шина.Большинство современных чипсетов не поддерживают эту шину. **USB** –Universal Serial Bus–универсальная последовательная шина.Сейчас стала широко распространена,имеет большие перспективы,сейчас уже есть стандартUSB2.

IDE –Integrated Device Electronic–устройства с интегрированным контроллером.Данная шина используется для подключения накопителей на жестких дискахCD-ROMиDVD-ROM приводах.

HI - Hub Interface–непереводимая игра слов(Hub –узел или центр чего либо),когда начали появляться новые быстрые периферийные устройства, РСстала не справляться сих запросами– 2ATA100 – 200Мб/с – PCI–133Мб/с. В первые данная архитектура была применена в I82810. Вообще понятие HI относится только к чипсетам фирмы Intel у других производителей аналогичные интерфейсы имеют другие названия, хотя выполняют те же функции и имеют вероятно похожие протоколы (к сожалению в обще доступных документах нет описания этих протоколов). У VIA аналогичный протокол назван V-Link интерфейс.

FWHI – Firm Ware Hub Interface (Узловой интерфейс для встроенного программного обеспечения-BIOS),после отказа отISAинтерфейса встала задача как загрузитьBIOSи была легкорешена с помощью выше описанного интерфейса. Нужно отметить, что в чипсетах от VIA нет такого интерфейса и BIOS грузится по LPC интерфейсу.

LPC – Low Pin Count Interface (Интерфейс малого количества контактов)действительно интерфейс имеет всего7контактов: 4для данных и3управляющих.Используется для подсоединения МІО у Intel и для BIOS у VIA,SIS.

AC97 -стандартный интерфейс для работы с внешним цифро-аналоговым или аналого-цифровым преобразователем,именно на его основе работают встроенные звуковые карты и дешевые модемы.

Порядок выполнения работы:

Ознакомится с программой Checkit для этого:

Запустить программу Checkit;

Ознакомившись с пунктом главного меню, записать в таблицу¹ какие элементы материнской платы можно тестировать с помощью программы.

Таблица 1

Название пункта меню	Наименование системы МВ, тестируемой в данном пункте

Тестирование основных элементов материнской платы.

Выполнить тестирование основных элементов материнской платы (центральный процессор, арифметический сопроцессор, контроллеры прерываний и прямого доступа к памяти) для этого:

Запустить программу Checkit;

В главном меню выбрать пункт «Тесты (Tests)» и подпункт «Плата ("System Board")».

Выполнить тестирование опорного генератора и часов реального времени для этого:

Запустить программу Checkit;

• В главном меню выбрать пункт «Тесты» и подпункт «Часы/таймер ("Real-Time Clock")». По окончании тестирования на экран выдается сводная таблица результатов проверки.

Выполнить тестирование параллельного порта для этого:

Выключить ПК;

Установить технологическую заглушку на параллельный порт; Включить ПК

Запустить программу Checkit;

В главном меню выбрать пункт «Тесты» и подпункт «Параллельный порт (Parallel Ports)».

Выбрать одно из логических имен параллельного порта, которые откроются в соответствующем подменю.

После выбора порта (LPT1) требуется указать имеются ли внешние подключения к порту "У-да, N-нет". Нажатие на клавиши N, соответствующей подключению к порту заглушки, начинает выполняться тест параллельного порта, который состоит из теста регистра данных и теста петли связи (заглушка закорачивает вход с выходом параллельного порта, т.е. выдаваемые портом сигналы им самим же и принимаются). После прохождения каждого из этих тестов, на против ставится соответствующее сообщение, а в окнах "ввод" и "вывод" выводятся данные, которые совпадают, если тест регистра данных исправен, и не совпадают в противном случае. Если есть, какие либо ошибки, то они выводятся на экран при нажатии на любую клавишу.

Выполнить тестирование последовательного порта для этого:

Выключить ПК;

Установить технологическую заглушку на последовательный порт; Включить ПК

Запустить программу Checkit;

В главном меню выбрать пункт «Тесты» и подпункт «Последовательный порт («Serial Ports»)».

Выбрать одно из логических имен последовательного порта (COM1-COM4), которые откроются в соответствующем подменю.

После прохождения каждого из этих тестов, на против ставится соответствующее сообщение, а в окнах "ввод" и "вывод" выводятся данные, которые совпадают, если тест регистра данных исправен, и не совпадают в противном случае. Если есть, какие либо ошибки, то они выводятся на экран при нажатии на любую клавишу.

Выполнить тестирование регистров устройств ввода информации для этого:

Запустить программу Checkit;

В главном меню выбрать пункт «Тесты» и подпункт «Устройства ввода ("Input Devices")».

Последовательно выполнить тестирование регистров клавиатуры и манипулятора типа мышь.

Контрольные вопросы.

Какие основные элементы расположены на материнской плате и каково их назначение? Какие виды неисправностей материнской платы существуют?

Какие способы диагностики неисправностей материнской платы существуют?

Какие элементы материнской платы можно диагностировать с помощью программы Checkit?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 6,7

Тестирование компонентов МВ с помощью POST – платы

Цель: Изучить методику тестирования компонентов МВ с помощью POST – платы. Получить навыки поиска неисправностей МВ с помощью POST – платы

Оборудование: ПК, Плата POST, программное обеспечение debug.exe. Расшифровка POST-кодов.

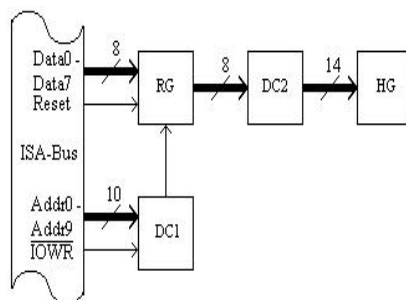
Порядок выполнения работы

Теоретические сведения

Устройство POST-платы

Плата-тестер PC-POST предназначена для мониторинга POST-кодов (POST - Power On Self Test / самотестирование по включению питания), посылаемых в порт ввода-вывода 80h программой BIOS на этапе самотестирования.

Плата POST состоит из четырех основных блоков:



RG - восьмиразрядный параллельный регистр; предназначен для записи и хранения очередного поступившего значения POST-кода;

DC1 - дешифратор разрешения записи в регистр; сигнал на выходе дешифратора становится активным в случае появления на адресной шине адреса диагностического регистра, а на шине управления - сигнала записи в устройства ввода-вывода;

- DC2 - дешифратор-преобразователь двоичного кода в код семисегментного индикатора;
- HG - двухразрядный семисегментный индикатор; отображает значение
- кода ошибки в виде шестнадцатеричных символов - 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, b, C, d, E, F.

Принцип работы POST Card PCI

При каждом включении питания компьютера, совместимого с IBM PC, и до начала загрузки операционной системы процессор компьютера выполняет процедуру BIOS под названием "Самотест по включению питания" - POST (Power On Self Test). Эта же процедура выполняется также при нажатии на кнопку RESET или при программной перезагрузке компьютера. Основной целью процедуры POST является проверка базовых функций и подсистем компьютера (таких как память, процессор, материнская плата, видеоконтроллер, клавиатура, гибкий и жесткий диски и т. д.) перед загрузкой операционной системы. Перед началом каждого из тестов процедура POST генерирует так называемый POST код, который выводится по определенному адресу в пространстве адресов устройств ввода/вывода компьютера. В случае обнаружения неисправности в тестируемом устройстве процедура POST просто "зависает", а предварительно выведенный POST код однозначно определяет, на каком из тестов произошло "зависание". Таким образом, глубина и точность диагностики при помощи POST кодов полностью определяется глубиной и точностью тестов соответствующей процедуры POST BIOS'a компьютера.

Следует отметить, что таблицы POST кодов различны для различных производителей BIOS и, в связи с появлением новых тестируемых

устройств и чипсетов, несколько отличаются даже для различных версий одного и того

производителя BIOS.

Для отображения POST кодов в удобном для пользователя виде служат устройства под названием POST Card.

В данной POST-карте (Рис.2) после включения питания компьютера (или нажатия на кнопку RESET) и до появления первого POST кода на индикатор POST-карты выводится специальный символ (Рис.3), который свидетельствует об отсутствии вывода компьютером каких-либо POST кодов. Это облегчает диагностику и позволяет наглядно определить, стартует ли компьютер вообще. Кроме того, этот же символ выводится при программном сбросе PCI шины для фиксации прохождения короткого сигнала RST

нажатия

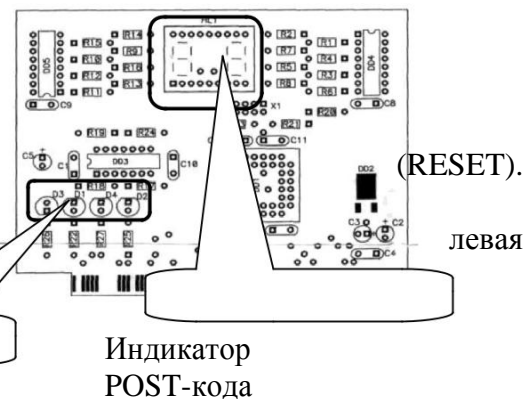


Рис.2 Размещение элементов POST-платы

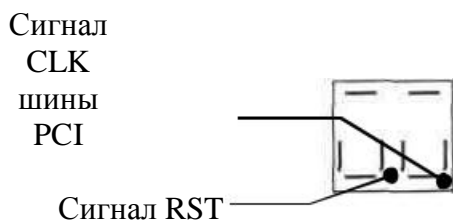


Рис.3 Внешний вид специального символа

Порядок выполнения работы:

Ознакомится с устройством POST-платы для этого:

Зарисовать внешний вид специального символа и месторасположение индикаторов сигналов RST и CLK шины PCI;

Зарисовать расположение индикатора питания и записать наличие, каких напряжений они контролируют;

Изучить методику проверки работоспособности POST-платы для этого: 2.2.1. Выключить ПК

Установить в свободный PCI слот MB POST-плату; Включить ПК и выполнить загрузку ОС

Запустить программу debug.exe

Используя команды программы debug.exe (I, O) выполнить запись в порт POST платы (80h) произвольных данных. Проконтролировать правильность считывания данных из порта POST платой. Контроль осуществлять по индикатору платы.

Изучить методику поиска неисправностей MB ПК для этого:

Выключить компьютер, произвести снятие всех плат расширения и банков памяти, отсоединить все внешние кабели, оставив только разъем питания.

.Установить в слот расширения POST-плату.

Включить ПК и производя последовательно установку снятых элементов и подключение внешних кабелей. **Установку снятых элементов производить при выключенном питании ПК:**

Модулей памяти Видеоадаптера Разъем монитора Разъем клавиатуры

Заполнить таблицу1.

Таблица 1

/п	Наименование установленных элементов	Звуковые сигналы POST	Сигналы и код, отображаемые платой POST	Расшифровка кода ошибки

Контрольные вопросы:

Каково назначение элементов POST-карты и используемый порт ввода вывода?

Каков алгоритм выполнения POST программы?

Какой метод поиска неисправностей материнской платы?

После включения питания компьютер —оживает только после неоднократного нажатия кнопки —RESET. Назовите возможные причины неисправности и способы их устранения?

При включении компьютера загорается светодиод Power, но ПК не работает. Проверка ЦП и мс памяти показала их исправность. Назовите возможные причины неисправности и способы их устранения?

При включении компьютера загорается светодиод Power, слышен звук вращения жёсткого диска и движения головок. Однако больше ничего не происходит. Опишите последовательность действий при определении неисправности с помощью диагностической карты и способы её устранения?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 8

Методы тестирования и ремонта аппаратной части НЖМД

Цель: Изучить методику тестирования и ремонта аппаратной части НЖМД.

Оборудование: ПК, программа, НЖМД.

Порядок выполнения работы

Ознакомиться с ремонтом HDD методом перекомпоновки для этого: • Соблюдая аккуратность снять электронную схему HDD;

проверить сопротивление обмоток (фаз) шпиндельного двигателя, которое должно составлять примерно 2 Ом. Записать полученные результаты;

- Выполнить замену электронной схемы HDD, взятой с аналогичного накопителя

Подать питающие напряжения на HDD, используя вольтметр проверить поступление питающих напряжений на HDD (измерение производить на разъеме питания подключенного к HDD);

- Убедиться, что при подаче питающих напряжений на HDD, происходит запуск двигателя привода диска и выполняется его начальная инициализация.

Ознакомиться с методом программного «ремонта» НЖМД

Выполнить подключение тестируемого HDD к системе для этого: Выключить ПК; Выполнить отключение установленного в ПК НЖМД. (НЖМД не снимать)

Подключить тестируемый НЖМД к системе; Включить ПК;

Ознакомиться с методами программного восстановления HDD для этого:

Выполнить загрузку ПК в режиме ДОС и запуск программы victoria 3.3.2.exe

Нажав клавишу **F1**, ознакомиться с основными командами программы и порядком их вызова записать назначение клавиш F1-F9;

Нажать клавишу «**P**» - и выбрать порт к которому подключен накопитель;

Нажав **F2** выполнить инициализацию исследуемого диска (данную команду следует выполнять перед выполнением любой команды) записать параметры диска- серийный номер, объем, CHS параметры, объем кэш памяти;

Нажав клавишу **F9**, вывести SMART таблицу диска, записать значения параметров (Val- относительное значение параметра, Worst-наихудшее когда-либо зафиксированное значение параметра; Trest-предельное значение параметра; Raw- абсолютное значение параметра):

Reallocated sector count и **Reallocated event count**: число переназначенных секторов;

Raw read error rate: количество ошибок чтения.

Current Pending Sector: отражает содержимое «временного» дефект-листа, т.е. текущее количество нестабильных секторов;

Uncorrectable Sector: показывает количество секторов, ошибки в которых не удалось скорректировать ECC-кодом. Если его значение выше нуля, это означает, что винту пора делать ремап;

Нажать клавишу **R** – выполнить измерение скорости вращения диска, записать полученное значение,

Нажать **F4**, и задав значение –линейное чтение и Ignore Bad Blocks, нажав F4 второй раз, запустить сканирование поверхности диска. Выполнить анализ полученных результатов, обратив внимание на количество вед блоков;

Нажав клавишу перейти в режим командной строки и ввести команду RNDVAD искусственно создать 10-20 soft-bad блоков. Создание soft-bad прерывается клавишей «**Esc**»;

Нажать **F4**, и задав значение –линейное чтение и «**Ignore Bad Blocks**», нажав F4 второй раз, запустить сканирование поверхности диска убедится в появлении вед блоков.

Для удаления софт-бедов выполнить инициализацию НЖМД, нажав клавишу **F2**, и ввести команду **F4** и выбрав режим «**BB = Advanced REMAP -Улучшенный алгоритм ремаппинга**» запустить сканирование диска. Контролируя процесс ремаппинга записать адреса восстановленных секторов.

Нажать **F4**, и задав значение –линейное чтение и «**Ignore Bad Blocks**», нажав F4 второй раз, запустить сканирование поверхности диска убедится что вед блоки удалены.

Вывести **SMART** таблицу диска, проанализировать значения полученных параметров сравнив их с предыдущими параметрами.

Контрольные вопросы.

Какие основные элементы НЖМД расположенные в гермоблоке и их каково назначение?

Какие основные элементы НЖМД расположенные на электронной плате и их каково назначение? Каковы основные виды неисправностей аппаратной части НЖМД и каковы причины их возникновения? Каковы основные дефектов магнитных дисков НЖМД и каковы причины их возникновения?

Какова методика диагностирования НЖМД? Какова причина появления софт-бедов?

Какова причина возникновения адаптивных бедов?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 9,10
Методы восстановления ОС

Цель: Изучить методику восстановления ОС «Windows», освоить практические навыки восстановления работоспособности ОС.

Оборудование: ПК, стандартные средства восстановления ОС.

Теоретические сведения

Порядок выполнения работы:

Ознакомится с работой System Restore для этого:

Запустив видеоролик «Создание точки восстановления системы.avi», ознакомится с методикой создания точки восстановления.

Запустив программ «System Restore» создать точку восстановления («Пуск - Все программы -

Стандартные - Служебные – Восстановление системы); Выйти из программы.

• Выполнить установку «условно неисправной программы» (любой не большой программы из каталога дистрибутив).

Запустив программ «System Restore», используя созданную точку восстановления, восстановить систему. Убедится, что система восстановлена до исходного состояния. Проверить работы системы если ПК не загружается для этого перезагрузить ПК и в начале загрузки ОС нажать клавишу F8 и выбрать пункт «Последнюю удачную конфигурацию» (Last

Known Good Configuration).

Записать последовательность работы.

Ознакомится с работой системы Rollback Driver для этого:

Выполнить изменение (замену на заведомо «не родной») драйвер устройства (например, монитор, принтер, звуковая карта). Последовательно выполнить следующие действия -> Мой компьютер - > свойства -> оборудование -> диспетчер устройств -> выбранное устройство. Открыть закладку свойств выбранного устройства. Выбрать закладку драйвер – обновить. При запуске мастера обновления оборудования выбрать пункт установка из указанного места – указать «Не выполнять поиск. Я сам выберу нужный драйвер». Снять флаг с пункта «Отображать только совместимые устройства. В открывшемся окне выбрать любое устройство и установить не корректный драйвер. Перезагрузить систему. Убедится в неработоспособности устройства.

Выбрав пункт «Откатить» восстановить исходный драйвер. Перезагрузить систему, убедится в работоспособности устройства.

Изучить средства архивации системы для этого создать архив системных файлов

Для создания ее резервной копии. Выполнить следующие действия: Пуск -> Все программы -> Стандартные -> Служебные -> Архивация данных. Перейти на закладку —Архивация». Установить галочку возле «System State» для архивации системных файлов и реестра. Осуществить выбор места размещения архива. Выполнить архивацию.

Восстановить систему из резервной копии. Выполнить следующие действия: выполнить загрузку системы в защищенном режиме. Запустить программу архивации, выбрав пункт «Восстановление и управление носителем» осуществить выбор архива и выполнить восстановление системы из резервной копии.

Создание резервной копии реестра средствами программы «REGEDIT»

Выполнить создание резервной копии одной из ветви реестра (HKEY_LOCAL_MACHINE,

HKEY_CURRENT_USER , HKEY_CLASSES_ROOT, HKEY_CURRENT_CONFIG, HKEY_USERS) для этого:

Запустить программу «regedit»; Выбрать нужный раздел/подраздел;

В меню программы выбрать команду «Экспорт»; указать путь сохранения копии и имя файла.

Восстановление реестра из резервной копии реестра средствами программы «REGEDIT»

Выполнить восстановление реестра из резервной копии для этого:

Запустить программу «regedit»;

- В главном меню выбрать команду «Импорт» с указанием пути к импортируемому файлу или
- выполнив двойной щелчок Лкм по архивному файлу запустить reg-файл, подтвердив импорт в реестр:

Изучение команд консоли восстановления (Emergency Recovery Console). Запустить консоль восстановления для этого:

Установить в НОД загрузочный оптический диск с дистрибутивом Windows; Перезагрузить компьютер, выполнив загрузку с диска;

Нажав клавишу «R» на предложение системы, запустить консоль восстановления;

После запуска Консоли восстановления выбрать установленную операционную систему (если на компьютере установлены две или несколько систем) и войти в нее, используя пароль администратора, дождаться загрузки интерфейса командной строки;

Вводя команды в формате «**help** <команда>» изучить следующие команды консоли: «**copy**», «**fixboot**», «**fixmbr**», «**format**».

Записать формат использования команд.

Контрольные вопросы.

Какие основные причины сбоев ОС, и какие существуют средства восстановления ОС?

Когда следует создавать и какова последовательность создания диска аварийного восстановления (ASR)?

Какова последовательность установки консоли восстановления (ERC)?

Какие существуют средства резервного копирования реестра и как ими пользоваться?

Когда, для каких целей и каков порядок использования основных команд консоли восстановления «copy», «fixboot», «fixmbr», «format»?

Какова последовательность действий для восстановления системы при неправильной установке драйвера устройства?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 11

Тема: Методы тестирования и ТО НОД.

Цель: Изучить методику тестирования и ТО НОД, освоить практические ТО НОД.

Оборудование: ПК, НОД, программа тестирования НОД «CDAn.exe».

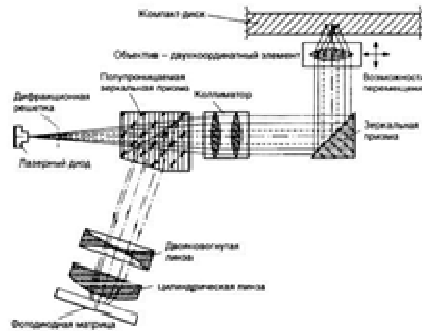
1. Теоретические сведения

Устройство НОД

Типовой привод НОД состоит из: платы электроники, шпиндельного двигателя, оптической системы считывающей головки системы загрузки диска.

Принцип работы НОД:

Полупроводниковый лазер генерирует маломощный инфракрасный луч, который попадает на отражающее зеркало. Серводвигатель по командам,



поступающим от встроенного микропроцессора, смещает подвижную каретку с отражающим зеркалом к нужной дорожке на компакт-диске. Отраженный от диска луч фокусируется линзой, расположенной под диском, отражается от зеркала и попадает на разделительную призму. Разделительная призма направляет отраженный луч на другую фокусирующую линзу. Эта линза направляет отраженный луч на фото датчик, который преобразует световую энергию в электрические импульсы. Сигналы с фотодатчика декодируются встроенным микропроцессором и передаются в компьютер в виде данных.

Наиболее часто встречаются следующие неисправности приводов CD-ROM.

• **Порядок выполнения работы:**

- Выполнить проверку правильности подключения НОД к системе для этого: Выключить ПК;
 - Выполнить смену канала IDE к которому подключен НОД и роль (MASTER-SLAVE);
- Восстановить исходное подключение; Включить ПК;

- Используя вольтметр проверить поступление питающих напряжений на НОД (измерение производить на разъеме питания подключенного к НОД);

Запустив программу «CDAn.exe», проверить качество считывания CD-диска, сняв зависимость скорости считывания от номера считываемого сектора. Зарисовать полученный график;

- Ознакомится с методикой ТО НОД для этого:
- Запустив видеоролик «Как очистить привод от осколков разорвавшегося диска» ознакомится с ним, обратив внимание на методику разборки НОД и чистки оптической системы.
- Выключить ПК; Снять НОД и выполнить его разборку, соблюдая при этом аккуратность;
- Используя пылесос и протирочный материал отчистить НОД от пыли и грязи; Выполнить смазку направляющей и шестерней редуктора НОД техническим вазелином (ЦИАТИМ) (не допуская при этом избытка смазки);
- Мягкой кисточкой осторожно очистить линзу от пыли. **Делать это надо с большой аккуратностью, чтобы не повредить подвеску лазера;**
- Осмотрев оптическую головку установить местонахождения резистора регулировки тока лазера. Записать назначение резистора и методику установки тока лазера; Собрать НОД и установить его в ПК; Включить ПК;

Запустив программу «CDAn.exe», проверить качество считывания CD-диска, сняв зависимость скорости считывания от номера считываемого сектора. Зарисовав полученный график, сравнить его с графиком, полученном при выполнении п. 2.1. Сделать выводы;

Контрольные вопросы и задания.

Из каких основных элементов состоит НОД? Указать их расположение.

Какова последовательность разборки НОД?

Каково назначение элементов оптической головки НОД?

Каковы основные типы неисправностей НОД и какова методика их устранения?

Какие системы автоматического регулирования (САР) существуют в НОД и каково их назначение?

Каков принцип работы САР НОД?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

сигналы (обычно на выводах микросхем и транзисторов) и делают заключение о возможных неисправных элементах.

6. Замена дефектных деталей. Производить замену деталей желательно на соответствующие схеме.

7. Анализ возможных причин неисправностей производится после завершения основных ремонтных работ на основании всей информации, полученной во время работы. Цель анализа — выявить основную причину отказа и сделать вывод о возможных отказах ВМ при дальнейшем его использовании.

8. Окончательная диагностика, настройка и тестирование производятся в комплексе с компьютером. В заключении рекомендуется провести так называемый "тепловой прогон" достаточно продолжительное время (не менее 2-х часов).

2. **Порядок выполнения работы:**

2.1. Знакомство с принципиальной схемой монитора

Ознакомится с принципиальной схемой монитора для этого:

- Используя принципиальную и структурную схему монитора выделить основные элементы монитора;
- Записать элементы, относящиеся к тракту обработки видеосигнала.
Используя шасси ВМ, ознакомится с размещением элементов на плате ВМ.

2.2. Ознакомится с критериями исправной работы тракта обработки видеосигнала для этого:

- Загрузить электронную модель тракта обработки видеосигнала 1.1.1. файл C:\.....\SURCUITS\Lab\CRT.ewb.

Ознакомится с расположением и назначением элементов управления модели:

Kabel- соединительный кабель ВМ-ПК

DIP – сигнальный разъем ВМ

RGB – мс. Видеоусилителя

VT1-VT3 – Выходные каскады видеоусилителя

CRT- ЭЛТ

BP блок питания

Измерительные вольтметры: U_c -измеряет сетевое напряжение, U_{p1} , U_{p2} -измеряют напряжение питание видеоусилителей, U_n - измеряет напряжение накала ЭЛТ, V_1 и V_2 в зависимости от положения переключателей U_m-U_{a1} , $U_{a2}-U_{a3}$ измеряют напряжение на электродах ЭЛТ.

Переключатели G-BR (2 шт) и B-R (2 шт) обеспечивают подключение генератора сигналов и осциллографа к каналам видеоусилителя.

2.3. Включить модель и ознакомится с критериями исправной работы тракта обработки видеосигналов RGB. Результаты занести в таблицу 1.

Таблица 1.

	Напряжен ие в	Признак исправности
--	------------------	------------------------

Элемент, параметр	Обозначение параметра	вольтах	тракта		
			R	G	B
Блок питания Сетевое напряжение	Uc				
Питающие напряжения	Up1 Up2 Um Ua1 Ua2 Ua3 Un				
Входная цепь	Амплитуда сигнала				
Mc видеоусилителя	Амплитуда сигнала				
Выходные видеоусилители	Амплитуда сигнала				

2.4. Ознакомится с методикой поиска неисправностей в тракте обработки видеосигнала для этого:

- Последовательно загружая модели C:\..... \SURCUITS\Lab\CRT1.ewb, C:\..... \SURCUITS\Lab\CRT2.ewb, C:\..... \SURCUITS\Lab\CRT3.ewb с введенными в них неисправностями, заполнить таблицу 2, 3, 4 (аналогичную таблице1).
- По результатам анализа данных в таблицах сделать выводы о предполагаемых неисправностях тракта и предложить метод ремонта.

2.5. Используя полученные данные составить общий алгоритм поиска неисправностей в тракте обработки видеосигнала.

Контрольные вопросы и задания.

Каково назначение основных элементов ВМ?

Указать расположение основных элементов ВМ.

Какие меры безопасности необходимо соблюдать при ремонте и диагностике ВМ и почему ?

Какова последовательность действий при поиске неисправностей в ВМ?

Каковы признаки исправной работы тракта обработки видеосигнала?

Какие виды сигналов подаются на вход ВМ и какова их характеристика?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А

Мельникова

Практическое занятие 13

Методика проведения ТО матричного принтера.

Цель: Изучить методику проведения ТО матричного принтера. Освоить методику составления алгоритма поиска неисправностей на узле подачи бумаги.

Оборудование: ПК, матричный принтер. Электронная модель тракта узла подачи бумаги.

1. Теоретические сведения

1.1. Устройство принтера

Типовая структурная схема принтера состоит из (Рис.1):

- Интерфейсный разъемы;
Источника питания;
- Основная логическая плата содержит:
 - Узел управления (микро ЭВМ, ЦП),
 - ОЗУ
 - Энергонезависимая память (ПЗУ),
 - ПЛИМ
 - Схема управления ШД каретки и узла подачи бумаги и
 - Схема управления ПГ
- Пульт управления содержит:
 - Индикаторы
 - Кнопки управления
- Печатающий механизм содержит:
 - ШД подачи бумаги
 - ШД каретки
 - ПГ
 - Датчи
 - Ки

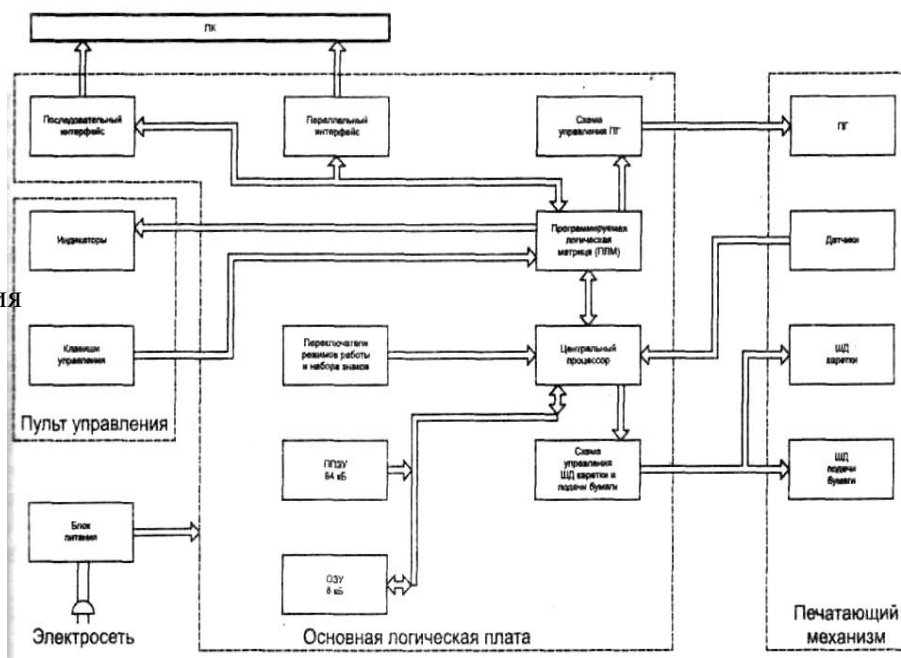


Рис. 1 Структурная схема матричного принтера

1.2. Профилактическое обслуживание принтера

Известно, что при правильной профилактике и эксплуатации принтера вероятность механических неисправностей принтера близка к нулю. Регулярная чистка принтера производится пылесосом и с последующей протиркой механических частей спиртом или бензином. Проверка принтера производится ежедневно и периодически.

Ежедневная проверка включает в себя:

- тестирование в режиме самотеста;
- ручное продвижение каретки в крайнее левое и правое положение;
- проверка работы картриджа с красящей лентой;
- проверка качества печати;
- проверка режимов подачи бумаги;
- проверка состояния ПГ.

После 6 месяцев эксплуатации принтера необходимо проводить периодическую проверку и смазку. Периодическая проверка включает в себя:

- проверка деформации троса или резинового шкива пошагового продвижения каретки;
- измерение зазора между ПГ и валиком;
- осмотр блок-контактов, датчиков, при необходимости их чистка;
- чистка ПГ;
- проверка механизма продвижения каретки и подачи бумаги;
- замена картриджа с красящей лентой или ленты;
- проверка исправности иголок ПГ.

Смазка механических узлов и деталей принтера осуществляется периодически, каждые 6 месяцев или после 1 миллиона отпечатанных знаков.

2. **Порядок выполнения работы:**

2.1. Используя видеofilm, ознакомится с методикой разборки и технического обслуживания матричного принтера.

2.2. **Отключить принтер от сети !**

2.3. Выполнить операции по разборке и ТО матричного принтера.

2.4. Подключить принтер к сети, включить его. Записать последовательность событий при инициализации принтера. Данные занести в таблицу 1.

Таблица 1

№ п/п	Элемент принтера	Действия, выполняемые при инициализации
1	Каретка ПГ	
2	Индикатор режима ON LINE	
3	Узел подачи бумаги	
4	Буфер принтера	
5	Зуммер принтера	

2.5. Ознакомится с критериями исправной работы тракта узла подачи бумаги для этого:

- Загрузить электронную модель тракта обработки видеосигнала 1.1.1. файл
C:\.....\SURCUIITS\Lab\Print.ewb.

- Ознакомится с расположением и назначением элементов управления модели:
 - drav- драйвер двигателя (набор ключевых транзисторов);
 - motor – шаговый двигатель узла подачи бумаги;
 - VT1-VT2 – транзисторы управления режимом работы двигателя «Стоп- Пуск» управляются ключом К1;
 - К2, К3 ключи подключения осциллографа к обмоткам двигателя.
- Установить переключатели в исходное положение:
 - К1-↓или ↑
 - К2-←
 - К2-←
- Включить модель и переключая переключатели, ознакомится с критериями исправной работы тракта.
 - Зарисовать полученные осциллограммы.
- Проанализировав схему узла тракта, составить алгоритм поиска неисправности узла.

Контрольные вопросы и задания.

Каково назначение основных элементов принтера?

Указать расположение основных элементов принтера.

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

Какова последовательность действий инициализации принтера?

Каковы признаки исправной работы тракта подачи бумаги?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 14,15

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 HP 1100.

1. Теоретические сведения

1.1. Устройство принтера

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 за счёт

электростатики на бумагу, на которой попадает 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 схема сканирования
7. Фузер- электрическая печка

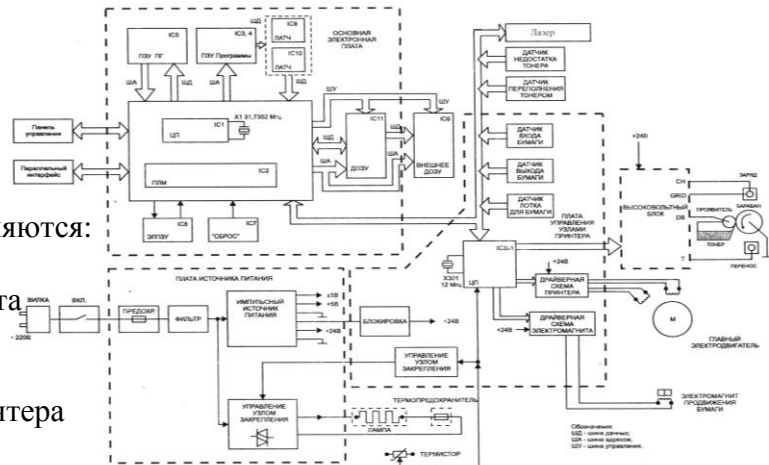


Рис. 1 Структурная схема лазерного принтера

2. **Порядок выполнения работы:**

2.1. Используя видеofilm, 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 на принтере
- 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 вынуть картридж, извлечь лист. Открыв защитный кожух фотобарабана проанализировать вид не закрепленного изображения и при наличии дефектов определить неисправный элемент.

2.3. **Отключить принтер от сети !**

2.4. Выполнить операции снятию картриджа лазерного принтера.

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

2.6. Выполнить замену элементов картриджа:

-
- Фотобарабана;
- магнитного вала;
-
-
-

чистящего лезвия;
дозировочного лезвия;
уплотнительного лезвия;
Собрать картридж и проверить его работоспособность, выполнив тест проверки вращения барабана

(Drum Rotation Test).

Контрольные вопросы и задания.

Каково назначение основных элементов принтера?

Указать расположение основных элементов картриджа принтера.

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

Каковы основные дефекты печати принтера и чем они обусловлены?

Как качество бумаги влияет на качество печати и почему?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 16

Техническое обслуживание клавиатуры и манипулятора типа мышь

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

Оборудование: ПК, клавиатура, манипулятор типа мышь.

1. **Теоретические сведения**

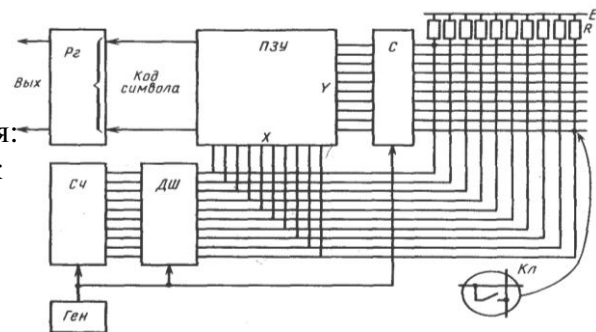
1.1. Устройство клавиатуры

Клавиатура предназначена для ввода алфавитно-цифровой информации и команд в ПК.

Основой клавиатуры является матрица контактов (клавиш). Клавиши могут выполняться в виде:

- резистивных датчиков, которые могут быть выполнены на основе:
 - о механических контактов
 - о пленочных контактов
 - герконовых контактов
- емкостных датчиков

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
- Дешифратор
- ПЗУ
- селектор Выходной регистр

Связь клавиатуры с ПК осуществляется последовательным

кодом.

1.2. Устройство мыши

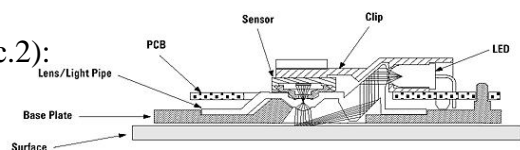
Механическая мышь состоит из:

- стальной обрезиненный шарик
- два пластмассовых валика с дисками
- микросхема управления с интерфейсом RS-232, PS/2, USB (в зависимости от мыши) и контроллером
- ролик для скроллинга (прокрутки)
- микровыключатели 2-3 шт. (в основном, хотя бывает и больше)

Принцип работы мыши заключается в следующем: катая мышь по столу, мы перемещаем шарик, шарик касается валиков с дисками, через отверстия которых информация поступает на фотоприемники. Информация их фотоприемников 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)



Ms обработки сигналов (Image Processor — процессор обработки изображений (DSP)).

Рис. 2 Устройство оптической мыши

Принцип работы оптической мыши заключается в следующем: 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 вычисляет результирующие показатели, свидетельствующие о направлении перемещения мыши вдоль осей X и Y, и передает результаты своей работы вовне по последовательному порту.

1.3. Профилактическое обслуживание клавиатуры и мыши.

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 обламываются рядом с корпусом мышки или рядом с её разъёмом. Определит место обрыва можно с помощью тестера или с помощью шевеления кабеля одной рукой, а мыши другой.

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

Сложнее при повреждении кабеля около разъёма так как он неразборный. Можно взять кабель с разъёмом, с какой-нибудь мыши или поискать новый разъём.

2. Порядок выполнения работы:

2.1. Используя видеофильм, ознакомится с методикой ТО (чистки) клавиатуры и мыши. Записать последовательность выполняемых операций.

2.2. Отключив клавиатуру и мышь от ПК выполнить последовательно основные сервисные процедуры для ТО клавиатуры и мыши.

2.3. Запустив тестовую программу «Dr. Hardware 2007 English version» проверить правильность формирования клавиатурой кода нажатой клавиши.

2.4. Выполнить операции по прозвонки соединительного кабеля мыши. Используя условные обозначения зарисовать схему соединения разъемов кабеля.

2.5. Используя омметр проверить работоспособность кнопок мыши.

Контрольные вопросы и задания.

Каково назначение клавиатуры и манипулятора типа мышь?

Каково назначение элементов контроллера клавиатуры?

Какова особенность организации интерфейса связи с ПК клавиатуры и манипулятора типа мышь?

Каковы достоинства и недостатки основных типов клавиатуры?

Каков принцип работы оптической мыши?

Каковы причины самопроизвольного перемещения указателя для оптической мыши?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 17,18

Прокладка кабеля и монтаж сетевых коробов, сетевых розеток

Цель:

- Изучить основные этапы монтажа кабельных систем Ethernet.
- Отработать навыки монтажа сети на основе витой пары.

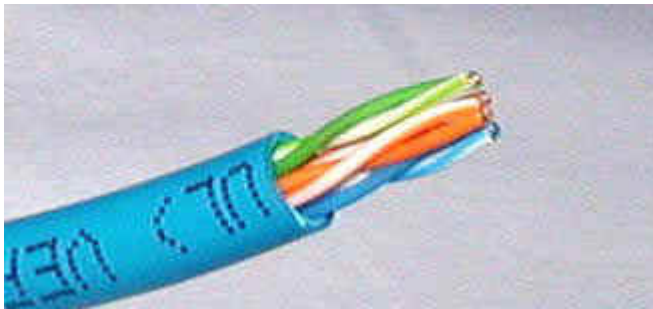
Оснащение: МУ к ПЗ, ПК

Теоретическая часть

Нарезка, зачистка и сортировка жил



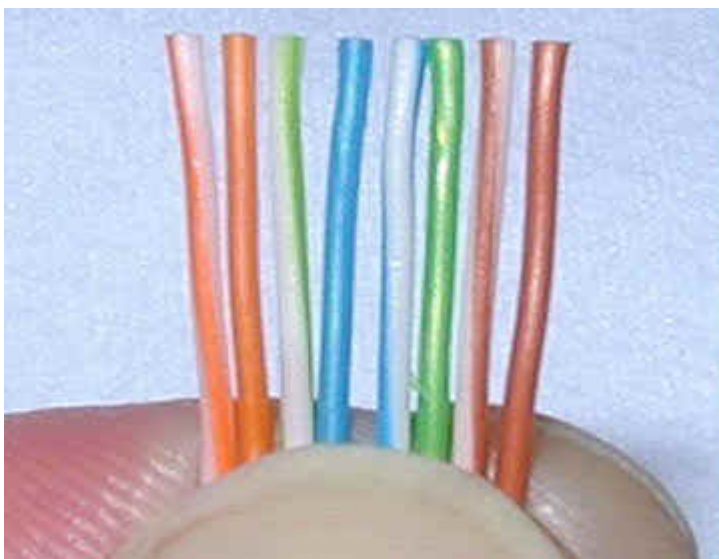
Снимите оплетку примерно на один дюйм (2,5 см). Некоторые обжимные инструменты (например, показанный в статье) имеют специальные лезвия для снятия оплетки. Вы вставляете кабель до упора (с другой стороны инструмента есть ограничитель) для того чтобы зачистить необходимую длину. Важно при этом не задеть сами жилы кабеля, перезание одной из восьми жил приведет к неработоспособности отрезка.



Некоторые производители витой пары экономят на цветной кодировке, и вам придется отслеживать пару, запоминая какой провод был связан с другим. Лучше всего проверить в магазине, чтобы цветная кодировка легко распознавалась. И чтобы потом не испытывать проблем и не мучаться, потратитесь на лучший кабель.

Б	О	Б	Г	Б	З	Б	К
Е	Р	Е	О	Е	Е	Е	О
Л	А	Л	Л	Л	Л	Л	Р
О	Н	О	У	О	Е	О	И
-	Ж	-	Б	-	Н	-	Ч
О	Е	З	О	Г	Ы	К	Н
Р	В	Е	Й	О	Й	О	Е
А	Ы	Л	Л			Р	В
Н	И	Е	У			И	Ы
Ж		Н	Б			Ч	Й
Е		Ы	О			Н	
В		Й	Й			Е	
Ы						В	
Й						Ы	
						Й	

Отсортируйте все жилы, затем убедитесь, чтобы они были прямыми и ровными. Срежьте несколько миллиметров, чтобы все проводки стали одной длины и выходили за изоляцию примерно на полдюйма (1,25 см).



Присоединение RJ-45 коннектора

Лучший способ вставки кабеля в RJ-45 коннектор.

- Держите коннектор пластиковой защелкой от себя.
- Когда сжимаете кабель для того чтобы вставить в коннектор, проследите, чтобы оболочка не болталась на проводках. Вставляйте отсортированные и выровненные жилы осторожно и

постепенно. Вы почувствуете сопротивление, как только жилы начнут попадать в пазы внутри коннектора.

- Посмотрите внимательно, чтобы жилы оставались в нужной последовательности. Иногда при вставке кабеля в коннектор в последний момент жилы могут поменяться местами. Используйте лупу если это необходимо.
- Протолкните жилы до конца коннектора, убедитесь, что все жилы одной длины и касаются прозрачной стенки. Вы должны видеть линию, состоящую из восьми концов жил. Если какая-то жила прошла не до конца, вынимайте кабель, выравнивайте жилы и пробуйте снова.
- Теперь засуньте оболочку кабеля как можно дальше в коннектор.

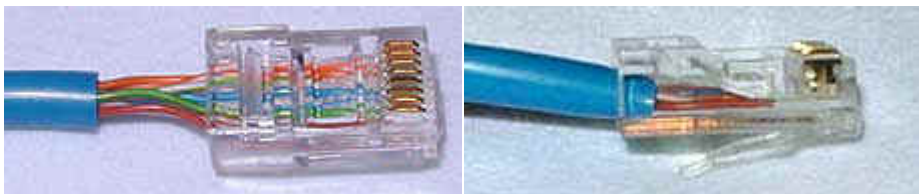


Обратите внимание на то, как изоляционная оболочка должна проходить в коннектор, и как все жилы упираются в конец коннектора.

Ниже приведу два примера как это не должно выглядеть. На примере слева оставлены слишком длинные жилы, из-за чего расстояние от коннектора до оплетки остается незащищенным. Также кабель теряет прочность.

На втором примере жилы срезаны слишком коротко, оплетка входит в коннектор, но длина концов не позволяет создать контакт с коннектором.

Неправильно:



Перед обжимом последний раз убедитесь что все жилы выровнены и проходят до конца. Теперь вставляйте коннектор в соответствующий зажим на инструменте, зажимайте рукоятки плавно прилагая усилие, но так чтобы не поломать коннектор. После обжима осмотрите коннектор, все контакты должны быть одной длины и утоплены в пластик.



Теперь повторите все процедуры со вторым концом кабеля. Используйте те же схемы как на первом коннекторе, тем самым закончив приготовление Straight-through (прямо проходящего, использующего хаб) кабеля.

Cross-over ("нуль хабный")

Теперь рассмотрим второй тип кабеля для соединения двух компьютеров между собой напрямую. Отличия этого вида от первого в том, что второй конец кабеля имеет другие цветовые схемы.

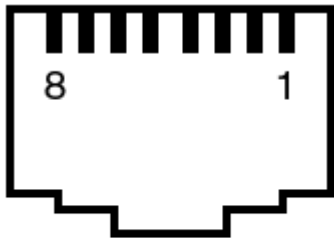
Первый конец, который будет идентичен Straight-through кабелю:

Б	О	Б	Г	Б	З	Б	К
Е	Р	Е	О	Е	Е	Е	О
Л	А	Л	Л	Л	Л	Л	Р
О	Н	О	У	О	Е	О	И
-	Ж	-	Б	-	Н	-	Ч
О	Е	З	О	Г	Ы	К	Н
Р	В	Е	Й	О	Й	О	Е
А	Ы	Л	Л	У	И	Р	В
Н	И	Е	У	У	И	Ы	
Ж		Н	Б	О	Ч	Й	
Е		Ы	О	И	Н	Е	
В		Й	И	И	В	Ы	
Ы					Ы	И	

Второй конец будет сделан по следующей схеме:

Б	З	Б	Г	Б	О	Б	К
Е	Е	Е	О	Е	Р	Е	О
Л	Л	Л	Л	Л	А	Л	Р
О	Е	О	У	О	Н	О	И
-	Н	-	Б	-	Ж	-	Ч
З	Ы	О	О	Г	Е	К	Н
Е	Й	Р	Й	О	В	О	Е
Л		А	Л	У	Ы	Р	В
Е		Н	У	И	И	Ы	
Н		Ж	Б	О	Ч	Й	
Ы		Е	О	И	Н	Е	
И		Ы	И	И	В	Ы	

А если быть точнее, то вот разводка для 10BaseT Crossover кабеля по номерам жил:



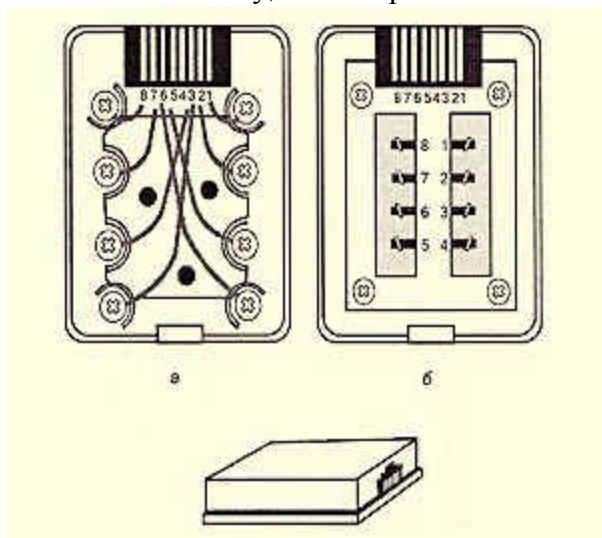
**RJ45 Male Plug
(on Cable)**

10BaseT Crossover Cable	
RJ45 #1 Pin	RJ45 #3 Pin
1 TX_D1+	3 RX_D2+
2 TX_D1-	6 RX_D2-
3 RX_D2+	1 TX_D1+
6 RX_D2-	2 TX_D1-

Если вы внимательно посмотрите на два конца Cross-over кабеля, то заметите, что разница всего лишь в том, что зеленая и оранжевая пара поменялись местами, а именно меняются 1-ый с 3-им и 2-ой с 6-ым.

Монтаж сетевых розеток

Сетевые розетки под «витую пару» представляют собой пластмассовый короб со съемной крышкой, в верхней части которого смонтирована ответная часть разъема RJ-45, оснащенная восемью подпружиненными контактами, а также имеется то или иное приспособление для подключения проводников сетевого кабеля. Обычно розетка имеет либо специальный клеящий слой, либо отверстия под винты для крепления ее к стене. Если развернуть розетку разъемом к себе таким образом, чтобы контакты оказались внизу, то номера контактов отсчитываются с 1 по 8 справа налево.



Сетевая розетка RJ-45

Так же, как и сам кабель «витая пара», сетевые розетки различаются по категориям, наиболее распространенными из которых являются категория 3 (рис. а) и категория 5 (рисунок, б). В сетевых розетках категории 3 проводники «витой пары» обычно крепятся к контактным площадкам с помощью винтов, что не обеспечивает требуемой надежности соединения. Для монтажа кабеля в таких розетках проводники «витой пары» необходимо расплести на необходимую длину, освободить от изоляции и, вставив в соответствующие контакты, зафиксировать прижимными винтами. При этом необходимо следить за тем, чтобы длина расплетенных проводников была не слишком большой, в противном случае между ними могут возникнуть паразитные наводки. Определить, какой провод «витой пары» должен идти к каждому из прижимных винтов, можно по номерам контактов разъема розетки: в целом схема подключения проводников должна соответствовать выбранной вами схеме заделки кабеля.

В более современных розетках категории 5 проводники витой пары просто вставляются в щели специальных контактных площадок, расположенных под углом в 90° к плоскости разъема RJ-45 (рис., б). При этом удаления защитного слоя с проводников не требуется: щели оснащены специальной режущей кромкой, которая сама прекрасно снимает с них изоляцию. Для надежной фиксации проводников в контактах розетки существует специальный инструмент, позволяющий поместить провод на максимальную глубину, однако в большинстве случаев можно прекрасно обойтись обыкновенным пинцетом и отверткой. Все контакты в розетках категории 5, как правило, пронумерованы, поэтому никаких проблем с разводкой кабеля возникнуть не должно.

Итак, общая последовательность монтажа сетевых розеток RJ-45 выглядит следующим образом.

1. Снимите крышку розетки, либо надавив на нее сбоку, либо поддев края крышки отверткой (в зависимости от устройства замка крышки).
2. Закрепите розетку на стене вблизи рабочего места либо на фиксирующих винтах, либо на клею.
3. Освободите от наружной изоляции оконечность идущего от розетки к концентратору кабеля «витая пара» на требуемую глубину и аккуратно расплетите проводники.
4. Присоедините проводники к контактам розетки согласно выбранной вами схеме заделки кабеля.
5. Закройте крышку розетки.
6. На противоположном от розетки конце кабеля «витая пара» смонтируйте разъем RJ-45, соблюдая выбранную вами схему заделки.

7. Проложите кабель до места крепления концентратора, фиксируя его через равные промежутки на плинтусе или на стене специальными крепежными скобами (их можно приобрести в любом магазине строительных товаров).

8. Подключите разъем RJ-45 в соответствующий порт концентратора.

Контрольные вопросы:

Виды кабелей для сетей (коаксиальный , неэкранированная витая пара, оптоволокно).

Устройства соединения BNC, RJ -45, настенные и модульные розетки, терминаторы.

EIA/TIA-568 Commercial Building Telecommunications Wiring Standard

Cross-over

Монтаж сетевых розеток

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 19

Создание сети между двумя ПК с помощью кабеля «витая пара»

Цель работы: Изучить основные топологии сетей и стандарты линий связи, выявить достоинства и недостатки линий связи локальных сетей, научиться проектировать локальные сети.

Оборудование: персональный компьютер, Microsoft Windows

Ход работы:

1. **Изучить теоретические сведения.**

Основные понятия

Типы линий связи локальных сетей

Средой передачи информации называются те линии связи (или каналы связи), по которым производится обмен информацией между компьютерами. В подавляющем большинстве компьютерных сетей (особенно локальных) используются проводные или кабельные каналы связи, хотя существуют и беспроводные сети, которые сейчас находят все более широкое применение, особенно в портативных компьютерах.

Каждый тип кабеля имеет свои преимущества и недостатки, так что при выборе надо учитывать как особенности решаемой задачи, так и особенности конкретной сети, в том числе и используемую топологию.

Можно выделить следующие основные параметры кабелей, принципиально важные для использования в локальных сетях:

1. Полоса пропускания кабеля (частотный диапазон сигналов, пропускаемых кабелем) и затухание сигнала в кабеле. Два этих параметра тесно связаны между собой, так как с ростом частоты сигнала растет затухание сигнала. Надо выбирать кабель, который на заданной частоте сигнала имеет приемлемое затухание. Или же надо выбирать частоту сигнала, на которой затухание еще приемлемо. Затухание измеряется в децибелах и пропорционально длине кабеля.

2. Помехозащищенность кабеля и обеспечиваемая им секретность передачи информации. Эти два взаимосвязанных параметра показывают, как кабель взаимодействует с окружающей средой, то есть, как он реагирует на внешние помехи, и насколько просто прослушать информацию, передаваемую по кабелю.

3. Скорость распространения сигнала по кабелю или, обратный параметр – задержка сигнала на метр длины кабеля. Этот параметр имеет принципиальное значение при выборе длины сети. Типичные величины скорости распространения сигнала – от 0,6 до 0,8 от скорости распространения света в вакууме. Соответственно типичные величины задержек – от 4 до 5 нс/м.

4. Для электрических кабелей очень важна величина волнового сопротивления кабеля. Волновое сопротивление важно учитывать при согласовании кабеля для предотвращения отражения сигнала от концов кабеля. Волновое сопротивление зависит от формы и взаиморасположения проводников, от технологии изготовления и материала диэлектрика кабеля. Типичные значения волнового сопротивления – от 50 до 150 Ом.

Кабели на основе витых пар

Витые пары проводов используются в дешевых и сегодня, пожалуй, самых популярных кабелях. Кабель на основе витых пар представляет собой несколько пар скрученных попарно изолированных медных проводов в единой диэлектрической (пластиковой) оболочке. Он довольно гибкий и удобный для прокладки. Скручивание проводов позволяет свести к минимуму индуктивные наводки кабелей друг на друга и снизить влияние переходных процессов.

Обычно в кабель входит две или четыре витые пары.

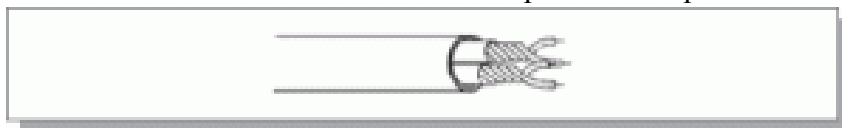


Рис. 5 – Кабель с витыми парами

Неэкранированные витые пары характеризуются слабой защищенностью от внешних электромагнитных помех, а также от подслушивания, которое может осуществляться с целью, например, промышленного шпионажа. Причем действие помех и величина излучения вовне увеличивается с ростом длины кабеля. Для устранения этих недостатков применяется экранирование кабелей.

В случае экранированной витой пары каждая из витых пар помещается в металлическую оплетку–экран для уменьшения излучений кабеля, защиты от внешних электромагнитных помех и снижения взаимного влияния пар проводов друг на друга. Для того чтобы экран защищал от помех, он должен быть обязательно заземлен. Естественно, экранированная витая пара заметно дороже, чем неэкранированная. Ее использование требует специальных экранированных разъемов. Поэтому встречается она значительно реже, чем неэкранированная витая пара.

Чаще всего витые пары используются для передачи данных в одном направлении (точка–точка), то есть в топологиях типа звезда или кольцо. Топология шина обычно ориентируется на коаксиальный кабель. Поэтому внешние терминаторы, согласующие неподключенные концы кабеля, для витых пар практически никогда не применяются.

Опволоконные кабели

Опволоконный (он же волоконно–оптический) кабель – это принципиально иной тип кабеля по сравнению с рассмотренными двумя типами электрического или медного кабеля. Информация по нему передается не электрическим сигналом, а световым. Главный его элемент – это прозрачное стекловолокно, по которому свет проходит на огромные расстояния (до десятков километров) с незначительным ослаблением.



Рис.7 – Структура оптоволоконного кабеля

Структура оптоволоконного кабеля очень проста и похожа на структуру коаксиального электрического кабеля. Только вместо центрального медного провода здесь используется тонкое (диаметром около 1 – 10 мкм) стекловолокно, а вместо внутренней изоляции – стеклянная или пластиковая оболочка, не позволяющая свету выходить за пределы стекловолокна. В данном случае речь идет о режиме так называемого полного внутреннего отражения света от границы двух веществ с разными коэффициентами преломления (у стеклянной оболочки коэффициент преломления значительно ниже, чем у центрального волокна). Металлическая оплетка кабеля обычно отсутствует, так как экранирование от внешних электромагнитных помех здесь не требуется. Однако иногда ее все–таки применяют для механической защиты от окружающей среды (такой кабель иногда называют броневым, он может объединять под одной оболочкой несколько оптоволоконных кабелей).

Оптоволоконный кабель обладает исключительными характеристиками по помехозащищенности и секретности передаваемой информации. Никакие внешние электромагнитные помехи в принципе не способны исказить световой сигнал, а сам сигнал не порождает внешних электромагнитных излучений. Подключиться к этому типу кабеля для несанкционированного прослушивания сети практически невозможно, так как при этом нарушается целостность кабеля. Стоимость оптоволоконного кабеля постоянно снижается и сейчас примерно равна стоимости тонкого коаксиального кабеля.

Однако оптоволоконный кабель имеет и некоторые недостатки:

1. Самый главный из них – высокая сложность монтажа (при установке разъемов необходима микронная точность, от точности скола стекловолокна и степени его полировки сильно зависит затухание в разьеме).

2. Использование оптоволоконного кабеля требует специальных оптических приемников и передатчиков, преобразующих световые сигналы в электрические и обратно, что порой существенно увеличивает стоимость сети в целом.

3. Оптоволоконные кабели допускают разветвление сигналов (для этого производятся специальные пассивные разветвители (couplers) на 2–8 каналов), но, как правило, их используют для передачи данных только в одном направлении между одним передатчиком и одним приемником.

4. Оптоволоконный кабель менее прочен и гибок, чем электрический.

5. Чувствителен оптоволоконный кабель и к ионизирующим излучениям, из-за которых снижается прозрачность стекловолокна, то есть увеличивается затухание сигнала.

6. Применяют оптоволоконный кабель только в сетях с топологией звезда и кольцо. Никаких проблем согласования и заземления в данном случае не существует. Кабель обеспечивает идеальную гальваническую развязку компьютеров сети. В будущем этот тип кабеля, вероятно, вытеснит электрические кабели или, во всяком случае, сильно потеснит их. Запасы меди на планете истощаются, а сырьё для производства стекла более чем достаточно.

Существуют два различных типа оптоволоконного кабеля:

1. многомодовый или мультимодовый кабель, более дешевый, но менее качественный;

2. одномодовый кабель, более дорогой, но имеет лучшие характеристики по сравнению с первым.

Суть различия между этими двумя типами сводится к разным режимам прохождения световых лучей в кабеле.



Рис.8 – Распространение света в одномодовом кабеле

В одномодовом кабеле практически все лучи проходят один и тот же путь, в результате чего они достигают приемника одновременно, и форма сигнала почти не искажается. Одномодовый кабель имеет диаметр центрального волокна около 1,3 мкм и передает свет только с такой же длиной волны (1,3 мкм). Дисперсия и потери сигнала при этом очень незначительны, что позволяет передавать сигналы на значительно большее расстояние, чем в случае применения многомодового кабеля. Для одномодового кабеля применяются лазерные приемопередатчики, использующие свет исключительно с требуемой длиной волны. Затухание сигнала в одномодовом кабеле составляет около 5 дБ/км и может быть даже снижено до 1 дБ/км.



Рис.9 – Распространение света в многомодовом кабеле

В многомодовом кабеле траектории световых лучей имеют заметный разброс, в результате чего форма сигнала на приемном конце кабеля искажается. Центральное волокно имеет диаметр 62,5 мкм, а диаметр внешней оболочки 125 мкм (это иногда обозначается как 62,5/125). Для передачи используется обычный (не лазерный) светодиод, что снижает стоимость и увеличивает срок службы приемопередатчиков по сравнению с одномодовым кабелем. Длина волны света в многомодовом кабеле равна 0,85 мкм, при этом наблюдается разброс длин волн около 30 – 50 нм. Допустимая длина кабеля составляет 2 – 5 км. Многомодовый кабель – это основной тип оптоволоконного кабеля в настоящее время, так как он дешевле и доступнее. Затухание в многомодовом кабеле больше, чем в одномодовом и составляет 5 – 20 дБ/км.

Типичная величина задержки для наиболее распространенных кабелей составляет около 4–5 нс/м, что близко к величине задержки в электрических кабелях.

Кроме кабельных каналов в компьютерных сетях иногда используются также бескабельные каналы. Их главное преимущество состоит в том, что не требуется никакой прокладки проводов (не надо делать отверстий в стенах, закреплять кабель в трубах и желобах, прокладывать его под фальшполами, над подвесными потолками или в вентиляционных шахтах, искать и устранять повреждения). К тому же компьютеры сети можно легко перемещать в пределах комнаты или здания, так как они ни к чему не привязаны.

Радиоканал использует передачу информации по радиоволнам, поэтому теоретически он может обеспечить связь на многие десятки, сотни и даже тысячи километров. Скорость передачи достигает десятков мегабит в секунду (здесь многое зависит от выбранной длины волны и способа кодирования).

Особенность радиоканала состоит в том, что сигнал свободно излучается в эфир, он не замкнут в кабель, поэтому возникают проблемы совместимости с другими источниками радиоволн (радио- и телевещательными станциями, радарными, радиолюбительскими и профессиональными передатчиками и т.д.). В радиоканале используется передача в узком диапазоне частот и модуляция информационным сигналом несущей частоты.

Главным недостатком радиоканала является его плохая защита от прослушивания, так как радиоволны распространяются неконтролируемо. Другой большой недостаток радиоканала – слабая помехозащищенность.

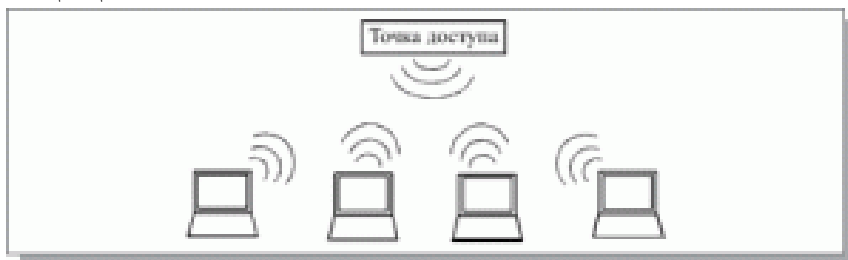


Рис. 10 – Объединение компьютеров

Радиоканал широко применяется в глобальных сетях как для наземной, так и для спутниковой связи. В этом применении у радиоканала нет конкурентов, так как радиоволны могут дойти до любой точки земного шара.

Инфракрасный канал также не требует соединительных проводов, так как использует для связи инфракрасное излучение (подобно пульту дистанционного управления домашнего телевизора). Главное его преимущество по сравнению с радиоканалом – нечувствительность к электромагнитным помехам, что позволяет применять его, например, в производственных условиях, где всегда много помех от силового оборудования. Правда, в данном случае требуется довольно высокая мощность передачи, чтобы не влияли никакие другие источники теплового (инфракрасного) излучения. Плохо работает инфракрасная связь и в условиях сильной запыленности воздуха.

Скорости передачи информации по инфракрасному каналу обычно не превышают 5–10 Мбит/с, но при использовании инфракрасных лазеров может быть достигнута скорость более 100 Мбит/с. Секретность передаваемой информации, как и в случае радиоканала, не достигается, также, требуются сравнительно дорогие приемники и передатчики.

Аппаратная часть локальных сетей

Аппаратура локальных сетей обеспечивает реальную связь между абонентами. Выбор аппаратуры имеет важнейшее значение на этапе проектирования сети, так как стоимость аппаратуры составляет наиболее существенную часть от стоимости сети в целом, а замена аппаратуры связана не только с дополнительными расходами, но зачастую и с трудоемкими работами.

К аппаратуре локальных сетей относятся:

1. кабели для передачи информации;
2. разъемы для присоединения кабелей;
3. согласующие терминаторы;
4. сетевые адаптеры;
5. репитеры;
6. трансиверы;
7. концентраторы.

О первых трех компонентах сетевой аппаратуры уже говорилось в предыдущих разделах, сейчас следует остановиться на функциях остальных компонентов.

Сетевые адаптеры

Сетевые адаптеры (они же контроллеры, карты, платы, интерфейсы, NIC – Network Interface Card) – это основная часть аппаратуры локальной сети. Назначение сетевого адаптера – сопряжение компьютера (или другого абонента) с сетью, то есть обеспечение обмена информацией между компьютером и каналом связи в соответствии с принятыми правилами обмена. Именно они реализуют функции двух нижних уровней модели OSI. Плата сетевого адаптера обычно имеет также один или несколько внешних разъемов для подключения к ней кабеля сети.

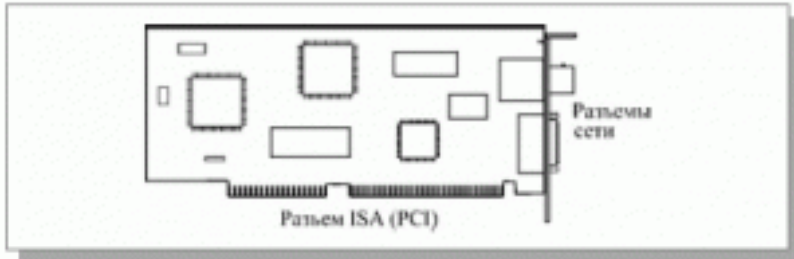


Рис. 11 – Плата сетевого адаптера

К основным сетевым функциям адаптеров относятся:

1. гальваническая развязка компьютера и кабеля локальной сети (для этого обычно используется передача сигналов через импульсные трансформаторы);
2. преобразование логических сигналов в сетевые (электрические или световые) и обратно;
3. кодирование и декодирование сетевых сигналов, то есть прямое и обратное преобразование сетевых кодов передачи информации (например, манчестерский код);
4. опознание принимаемых пакетов (выбор из всех приходящих пакетов тех, которые адресованы данному абоненту или всем абонентам сети одновременно);
5. преобразование параллельного кода в последовательный при передаче и обратное преобразование при приеме;
6. буферирование передаваемой и принимаемой информации в буферной памяти адаптера;
7. организация доступа к сети в соответствии с принятым методом управления обменом;
8. подсчет контрольной суммы пакетов при передаче и приеме.

Все остальные аппаратные средства локальных сетей (кроме адаптеров) имеют вспомогательный характер, и без них часто можно обойтись. Это сетевые промежуточные устройства.

Трансиверы или приемопередатчики

Трансиверы или приемопередатчики (от английского TRANsmitter + reCEIVER) служат для передачи информации между адаптером и кабелем сети или между двумя сегментами (частями) сети. Трансиверы усиливают сигналы, преобразуют их уровни или преобразуют сигналы в другую форму (например, из электрической в световую и обратно). Трансиверами также часто называют встроенные в адаптер приемопередатчики.

Репитеры

Репитеры или повторители (repeater) выполняют более простую функцию, чем трансиверы. Они не преобразуют ни уровни сигналов, ни их физическую природу, а только восстанавливают ослабленные сигналы (их амплитуду и форму), приводя их к исходному виду. Цель такой ретрансляции сигналов состоит исключительно в увеличении длины сети.

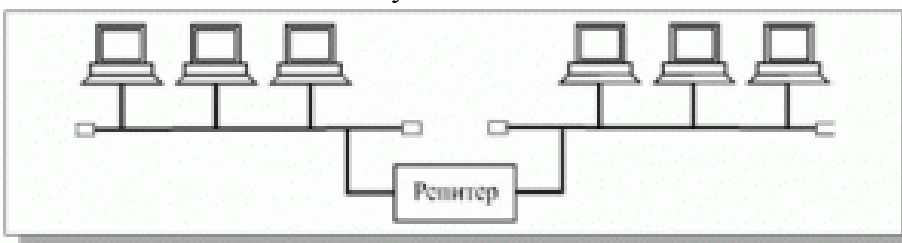


Рис. 12 – Соединение репитером двух сегментов сети

Концентраторы

Концентраторы (хабы, hub), как следует из их названия, служат для объединения в сеть нескольких сегментов. Концентраторы (или репитерные концентраторы) представляют собой несколько собранных в едином конструктиве репитеров, они выполняют те же функции, что и репитеры.

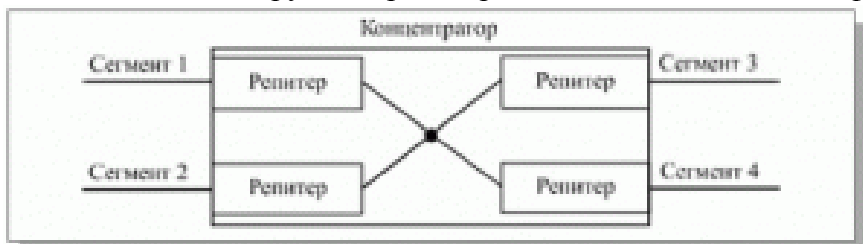


Рис. 13 – Схема концентратора

Преимущество подобных концентраторов по сравнению с отдельными репитерами в том, что все точки подключения собраны в одном месте, это упрощает реконфигурацию сети, контроль и поиск неисправностей. К тому же все репитеры в данном случае питаются от единого качественного источника питания.

Коммутаторы

Коммутаторы (свичи, коммутирующие концентраторы, switch), как и концентраторы, служат для соединения сегментов в сеть. Они также выполняют более сложные функции, производя сортировку поступающих на них пакетов.

Коммутаторы передают из одного сегмента сети в другой не все поступающие на них пакеты, а только те, которые адресованы компьютерам из другого сегмента. Пакеты, передаваемые между абонентами одного сегмента, через коммутатор не проходят. При этом сам пакет коммутатором не принимается, а только пересылается.

2. Построить схему сети университета и ее модель с указанием топологии сетей и стандартов линий связи.

. Основными критерием выбора должны быть: экономичность и достаточная пропускная способность. Сделать приблизительный расчет количества материалов и стоимости такой сети с учетом «сетевой» аппаратуры.

Исходные данные приведены в таблице.

Вариант 1

№ корпуса	Количество классов	Количество ПК в классе
1	12	15
2	10	
3	6	
4	8	

Вариант 2

№ корпуса	Количество классов	Количество ПК в классе
1	8	10
2	13	
3	9	

4	5	
---	---	--

Вариант 3

№ корпуса	Количество классов	Количество ПК в классе
1	4	19
2	17	
3	2	
4	1	

Вариант 4

№ корпуса	Количество классов	Количество ПК в классе
1	8	5
2	19	
3	12	
4	16	

Вариант 5

№ корпуса	Количество классов	Количество ПК в классе
1	12	2
2	20	
3	26	
4	18	

Объяснить, чем руководствовались при выборе тех или иных элементов сети и указать их преимущества, отразить результат и обоснование критериев выбора в отчете.

Контрольные вопросы

Какие топологии сетей вы знаете?

Чем отличается локальная сеть от глобальной?

Может ли быть компьютер одновременно клиентом и сервером?

Сколько проводов в витой паре?

Можно ли назвать соединение шина с соединенными концами – кольцом?

Чем отличается свитч (switch) от хаба (hub)?

Для чего нужен Терминатор?

Каково назначение сетевого адаптера?

Чем отличается витая пара в стандартах 100-BASE-T и 1000-BASE-T?

Чем обусловлена задержка в оптоволоконных и электрических кабелях?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 20

Создание сети с помощью беспроводных адаптеров

Цель: изучить технологию создания беспроводной сети

Оснащение: МУ к ПЗ, ПК

В современном мире все большее применение находят беспроводные сети Wi-Fi, позволяющие давать клиентам доступ к ресурсам сетей, например к **Internet**, с ноутбука или персонального компьютера, используя в качестве среды передачи данных радиоканал, что не требует наличия специальных проводных соединений клиентов с сетью, обеспечивая таким образом их мобильность.

Преимущества Wi-Fi

Отсутствие проводов. Передача данных в сети осуществляется по радиоканалу. Возможна установка в местах, где прокладка проводной сети по тем или иным причинам невозможна или нецелесообразна, например на выставках, залах для совещаний.

Мобильность, как рабочих мест, так и самого офиса. Так как беспроводная сеть не привязана к проводам, Вы можете свободно изменять местоположение Ваших компьютеров в зоне покрытия точки доступа, не беспокоясь о нарушениях связи. Сеть легко монтируется/демонтируется, при переезде в другое помещение Вы можете даже забрать свою сеть с собой

Недостатки Wi-Fi

Относительно высокая стоимость оборудования

Небольшая дальность действия – 50-100 метров

Велика опасность несанкционированного подключения к сети сторонних пользователей

В предлагаемой работе *мы освоим* создание простейшей сети Wi-Fi на примере подключения ноутбуков к точке доступа Wi-Fi с использованием статической и динамической IP-адресации.

Схема сети имеет следующий вид:



Монтаж сети.

1. Возьмите у преподавателя Wi-Fi-адаптер. Подключите адаптер к USB-порту **ноутбука №2**. (См. схему сети).

1. Включите ноутбуки. После загрузки операционной системы на ноутбуках, на обоих адаптерах должны загореться сигнальные лампочки, свидетельствующие о установке радиообмена между адаптерами и точкой доступа.

2. Сеть собрана, теперь ее необходимо настроить.

1-я часть работы. Настройка сети со статическим адресом компьютера клиента.

Настройка сети заключается в установке **протоколов ноутбука клиента**, которые необходимы для его работы, а так же включение и настройка **DHCP-сервера**, который находится в точке.

Запомните. **Протокол** – это специальная программа, посредством которой компьютеры сети обмениваются между собой данными по специальным правилам. В нашей сети рабочим протоколом будет протокол **TCP/IP**. Чтобы компьютеры могли обмениваться между собой данными этот протокол должен быть установлен на всех компьютерах, которые находятся в сети.

На **ноутбуке сервере** протокол TCP/IP уже установлен, нам осталось установить и настроить этот протокол на **ноутбуке клиенте** (см. схему сети). *Помните*, что все пункты настройки должны выполняться в той последовательности, в которой они указаны. Не нарушайте последовательность настройки.

Function Enable / Disable – Включает (Enabled) или отключает (Disabled) DHCP-сервер.

IPAssignedFrom – задает начальный IP-адрес, с которого начинается диапазон IP-адресов, выделяемых динамически пользователям (пользователи, которые подключаются временно).

TheRangeofPool – задает конец диапазона IP-адресов, конечное значение последней цифры IP-адреса.

Таким образом в нашем примере мы задали диапазон IP-адресов от **192.168.0.51** до **192.168.0.200** включительно.

SubMask – маска подсети. Это специальный параметр, который вместе с адресом однозначно определяет сеть, в которой находится компьютер.

LeaseTime – время «жизни» выделенных пользователю сетевых настроек. При динамической адресации настройки пользователя существуют определенное время, после чего сбрасываются и программное обеспечение пользователя запрашивает новые настройки. Здесь задается время существования выделенных пользователю настроек (в секундах).

Status – специальный параметр, он ставится в значение **ON**, если в сети используется совместно **динамическая** и **статическая** адресации. В нашем случае этот параметр установлен в **ON**, поскольку на **ноутбуке клиента** прописан статический, постоянный адрес.

Проверка работы беспроводной сети.

После того, как сеть настроена, нужно проверить ее работу и убедиться, что компьютеры могут обмениваться данными между собой. *Необходимо знать*, что в сети могут существовать самые разные службы и сервисы, каждый из которых выполняет свои задачи. В сети, которую мы настроили работают две службы: локальный **WEB-сервер**, предназначенный для размещения HTML-страниц в сети, и **Сеть Microsoft**, посредством которой производится обмен файлами и совместная работа с клиентами.

Сначала проверим работу **WEB-сервера**. **WEB-сервер** установлен на **ноутбуке сервер**. Для того, чтобы проверить работу **WEB-сервера**, запустите на **ноутбуке №2** (компьютер Клиент) обозреватель Интернета **Internet Explorer** и в его адресной строке введите <http://192.168.0.3/wifi/>

Если страница загрузится, действуйте в соответствии с указаниями, написанными на этой странице.

Если страница не загрузилась, значит сеть настроена неправильно. Тогда сделайте следующее:

1. Проверьте еще раз настройки протокола TCP/IP **ноутбука клиента** и убедитесь что они введены правильно.
 1. Если ошибка не исчезает, позвоните преподавателя.

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 21

Настройка локальной сети LAN в Kubuntu Linux.

Цель: настроить LAN в Kubuntu Linux.

Оснащение: МУ к ПЗ, ПК

Порядок выполнения работы

Настройка локальной сети в Kubuntu (далее Linux) с помощью графической утилиты мало чем отличается от настройки в Windows 7. Поэтому мы рассмотрим настройку с помощью консоли. Включите ноутбук и в появившемся меню выбора операционной системы загрузчика Grub выберите ОС Linux/Kubuntu/Ubuntu и дождитесь загрузки ОС.

Для запуска консоли нажмем **Alt+F2** в появившейся строке введем **konsole**. Откроется окно стандартный терминала графической среды KDE.

Выполним команду **ifconfig**, для чего наберем команду в терминале и нажмём клавишу **ENTER**:



```
notebook2@notebook2-K54L:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 54:04:a6:10:59:8a
          inet6 addr: fe80::5604:a6ff:fe10:598a/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8195 (8.1 KB)  TX bytes:17257 (17.2 KB)
          Interrupt:50

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436 Metric:1
          RX packets:484 errors:0 dropped:0 overruns:0 frame:0
          TX packets:484 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34928 (34.9 KB)  TX bytes:34928 (34.9 KB)

wlan0     Link encap:Ethernet  HWaddr 60:d8:19:12:5d:f6
          inet addr:192.168.137.100  Bcast:192.168.137.255  Mask:255.255.255.0
          inet6 addr: fe80::62d8:19ff:fe12:5df6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:7287 errors:0 dropped:0 overruns:0 frame:0
          TX packets:6192 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8718036 (8.7 MB)  TX bytes:867901 (867.9 KB)

notebook2@notebook2-K54L:~$
```

Состояние всех доступных сетевых интерфейсов, полученных командой **ifconfig**.

Команда покажет нам состояние всех доступных сетевых интерфейсов. **eth0** — интерфейс проводной сети.

lo — **loopback**, т. н. локальная петля. **wlan0** — интерфейс беспроводной сети

Для настройки(показа состояния) конкретного интерфейса необходимо указать его первым параметром команды `ifconfig`.

Простейшая настройка сетевого интерфейса сводится к установке `ip`-адреса и включению его. Выполним команду

```
sudo ifconfig eth0 192.168.1.xxx up
```

`sudo` — дает нам право на изменение параметров интерфейса (права суперпользователя `root` в Linux)

`eth0` — имя интерфейса.

192.168.1.xxx — `ip`-адрес, который мы хотим назначить (для первого ноутбука назначьте адрес **192.168.1.10**, а для второго **192.168.1.11**)

`up/down` — соответственно включить/выключить интерфейс.

Команда `sudo` попросит ввести пароль текущего пользователя — Для ноутбуков текущий пароль: **notebook** (вводимые символы пароля не отображаются в терминале).

В результате мы видим настроенные параметры LAN адаптера, введя команду **ifconfig eth0** после настройки интерфейса:



```
notebook2 : bash
Файл  Правка  Вид  Закладки  Настройка  Справка
notebook2@notebook2-K54L:~$ sudo ifconfig eth0 192.168.1.11 up
notebook2@notebook2-K54L:~$ ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 54:04:a6:10:59:8a
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::5604:a6ff:fe10:598a/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:106 errors:0 dropped:0 overruns:0 frame:0
          TX packets:126 errors:0 dropped:0 overruns:0 carrier:2
          collisions:0 txqueuelen:1000
          RX bytes:8195 (8.1 KB)  TX bytes:21318 (21.3 KB)
          Interrupt:50

notebook2@notebook2-K54L:~$
```

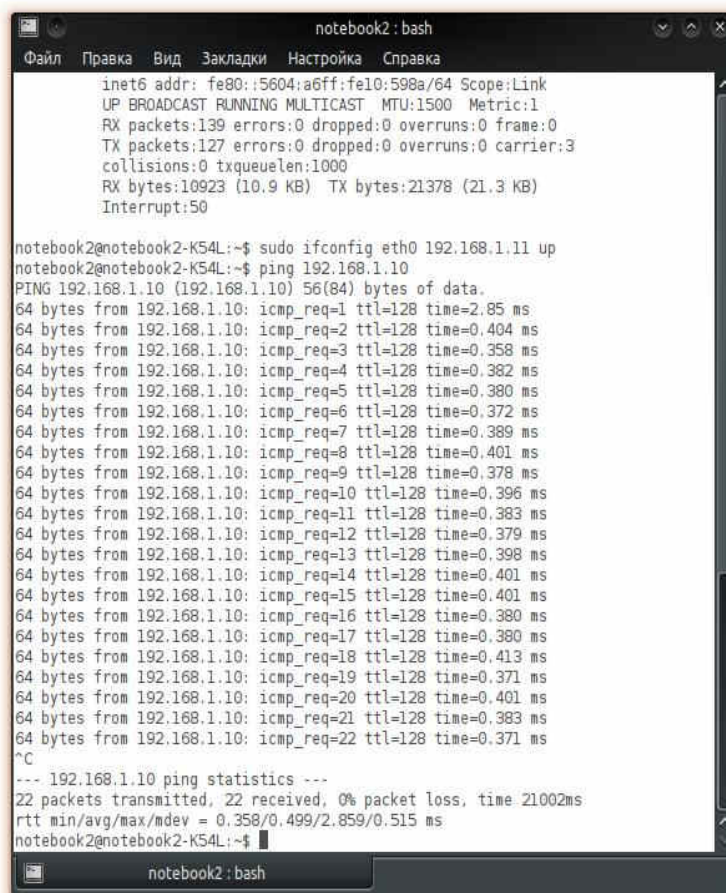
Результат выполнения команды **ifconfig eth0** после настройки LAN.

Теперь соединив соединив LAN порты ноутбуков сетевым кабелем (RJ45), можно проверить работу сети с помощью команды:

ping 192.168.1.11

Команда выполняется в консоли на ноутбуке с ip адресом **192.168.1.10** Таким образом мы проверяем доступность другого ноутбука по сети и правильность её работы.

При удачной настройке сети ее результат:



```
notebook2 : bash
inet6 addr: fe80::5604:a6ff:fe10:598a/64 Scope:Link
UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
RX packets:139 errors:0 dropped:0 overruns:0 frame:0
TX packets:127 errors:0 dropped:0 overruns:0 carrier:3
collisions:0 txqueuelen:1000
RX bytes:10923 (10.9 KB)  TX bytes:21378 (21.3 KB)
Interrupt:50

notebook2@notebook2-K54L:~$ sudo ifconfig eth0 192.168.1.11 up
notebook2@notebook2-K54L:~$ ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data:
64 bytes from 192.168.1.10: icmp_req=1 ttl=128 time=2.85 ms
64 bytes from 192.168.1.10: icmp_req=2 ttl=128 time=0.404 ms
64 bytes from 192.168.1.10: icmp_req=3 ttl=128 time=0.358 ms
64 bytes from 192.168.1.10: icmp_req=4 ttl=128 time=0.382 ms
64 bytes from 192.168.1.10: icmp_req=5 ttl=128 time=0.380 ms
64 bytes from 192.168.1.10: icmp_req=6 ttl=128 time=0.372 ms
64 bytes from 192.168.1.10: icmp_req=7 ttl=128 time=0.389 ms
64 bytes from 192.168.1.10: icmp_req=8 ttl=128 time=0.401 ms
64 bytes from 192.168.1.10: icmp_req=9 ttl=128 time=0.378 ms
64 bytes from 192.168.1.10: icmp_req=10 ttl=128 time=0.396 ms
64 bytes from 192.168.1.10: icmp_req=11 ttl=128 time=0.383 ms
64 bytes from 192.168.1.10: icmp_req=12 ttl=128 time=0.379 ms
64 bytes from 192.168.1.10: icmp_req=13 ttl=128 time=0.398 ms
64 bytes from 192.168.1.10: icmp_req=14 ttl=128 time=0.401 ms
64 bytes from 192.168.1.10: icmp_req=15 ttl=128 time=0.401 ms
64 bytes from 192.168.1.10: icmp_req=16 ttl=128 time=0.380 ms
64 bytes from 192.168.1.10: icmp_req=17 ttl=128 time=0.380 ms
64 bytes from 192.168.1.10: icmp_req=18 ttl=128 time=0.413 ms
64 bytes from 192.168.1.10: icmp_req=19 ttl=128 time=0.371 ms
64 bytes from 192.168.1.10: icmp_req=20 ttl=128 time=0.401 ms
64 bytes from 192.168.1.10: icmp_req=21 ttl=128 time=0.383 ms
64 bytes from 192.168.1.10: icmp_req=22 ttl=128 time=0.371 ms
^C
--- 192.168.1.10 ping statistics ---
22 packets transmitted, 22 received, 0% packet loss, time 21002ms
rtt min/avg/max/mdev = 0.358/0.499/2.859/0.515 ms
notebook2@notebook2-K54L:~$
```

Контрольные вопросы

- Какие топологии сетей вы знаете?
- Чем отличается локальная сеть от глобальной?
- Может ли быть компьютер одновременно клиентом и сервером?
- Сколько проводов в витой паре?
- Можно ли назвать соединение шина с соединенными концами – кольцом?
- Чем отличается свитч (switch) от хаба (hub)?
- Для чего нужен Терминатор?
- Каково назначение сетевого адаптера?
- Чем отличается витая пара в стандартах 100-BASE-T и 1000-BASE-T?
- Чем обусловлена задержка в оптоволоконных и электрических кабелях?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.
Преподаватель

Н.А Мельникова

Практическое занятие 22

Подключение и настройка клиента Windows 7

Цель: изучить подключение нового клиента в Windows 7

Оснащение: МУ к Пз

Краткие теоретические сведения

Сеть компьютер-компьютер представляет собой временное соединение компьютеров и устройств для определенной цели, например совместного использования документов во время встречи или компьютерной игры нескольких игроков. Можно временно установить общее подключение к Интернету в сети компьютер-компьютер, чтобы пользователям не пришлось настраивать собственные подключения.

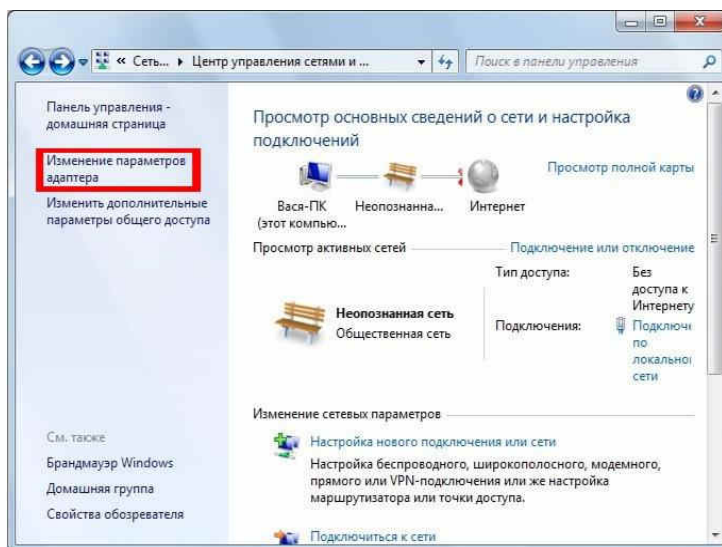
Порядок работы.

Включите оба ноутбука. В случае разряженной батареи подключите ноутбуки к сети 220 В через блок питания.

В появившемся меню выбора операционной системы загрузчика Grub выберите ОС Windows 7 и дождитесь загрузки ОС. С помощью LAN – тестера выберите правильно обжатую витую пару (RJ45). Соедините LAN порты ноутбуков сетевым кабелем (RJ45).

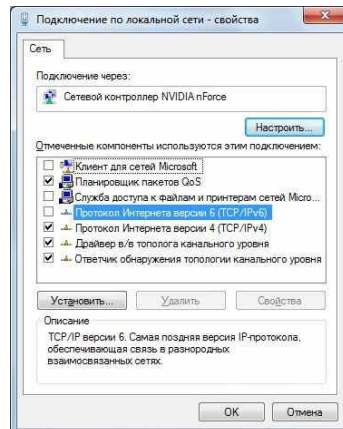
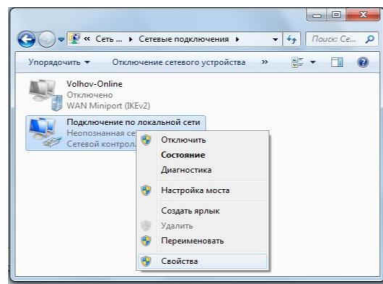
Для того чтобы настроить подключение по локальной сети вам необходимо зайти в меню «Пуск» (нижний левый угол экрана).

В появившемся меню выбрать «Панель управления» -> «Сеть и Интернет», затем «Центр управления сетями и общим доступом». В появившемся окне нажать на «Изменение параметров адаптера» (меню слева) рис. 5.1.



Центр управления сетями и общим доступом Windows 7.

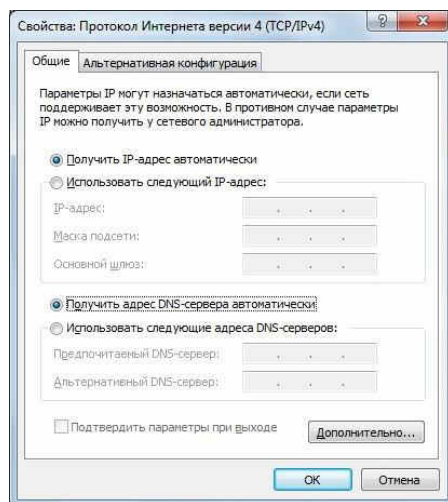
Правой кнопкой мыши нажать на «Подключение по локальной сети» и выбрать пункт «Свойства».



Настройка сетевой карты на Windows 7.

В появившемся диалоговом окне снять галочки с элементов «Клиент для сетей Microsoft», «Служба доступа к файлам и принтерам сетей Microsoft», «Протокол Интернета версии 6(TCP/IPv6)» рис. 5.3.

Далее необходимо выделить пункт «Протокол Интернета версии 4(TCP/IPv4)» и нажать кнопку «Свойства» рис. 5.4.



Протокол Интернета версии 4(TCP/IPv4)

Переведем радиокнопку в положение «Использовать следующий IP-адрес» и введем в поля следующие данные:

Для ноутбука №1:

IP-адрес	192.168.1.10
Маска подсети	255.255.255.0

Для ноутбука №2:

IP-адрес	192.168.1.11
Маска подсети	255.255.255.0

Оставшиеся поля оставим пустыми и нажмем кнопку ОК.

Настройка сетевого соединения между двумя ноутбуками завершена. Для проверки правильности необходимо выполнить следующие действия:

- Нажать комбинацию клавиш win + R
- Ввести в открывшееся окно cmd.exe
- В окне консоли выполнить команду ping 192.168.1.11 (для первого ноутбука) или ping 192.168.1.10 для второго. Если в результате появятся строки «Ответ от...», то настройка сети выполнена верно.

Контрольные вопросы

Какие топологии сетей вы знаете?

Чем отличается локальная сеть от глобальной?

Может ли быть компьютер одновременно клиентом и сервером?

Сколько проводов в витой паре?

Можно ли назвать соединение шина с соединенными концами – кольцом?

Чем отличается свитч (switch) от хаба (hub)?

Для чего нужен Терминатор?

Каково назначение сетевого адаптера?

Чем отличается витая пара в стандартах 100-BASE-T и 1000-BASE-T?

Чем обусловлена задержка в оптоволоконных и электрических кабелях?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 23 Настройка ActiveDirectory

Цель работы: приобретение студентами практических навыков установки и настройки Active Directory.

Оснащение: МУ к ПЗ, ПК

Общие сведения

Каталог представляет собой иерархическую структуру, которая хранит сведения об объектах в сети. Служба каталогов, такая как Active Directory, обеспечивает возможность хранения данных каталога и доступа к этим данным сетевых пользователей и администраторов. Например, в Active Directory хранятся сведения об учетных записях пользователей, такие как имена, пароли, номера телефонов и тому подобные, к которым могут получать доступ другие пользователи той же сети, прошедшие проверку

Служба каталогов - одна из наиболее важных составных частей развитой компьютерной системы. Пользователи и администраторы зачастую не знают точных имен нужных им объектов, которые им в данный момент требуются. Они могут знать один или несколько их признаков или атрибутов (attributes) и могут послать запрос (query) к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе. Служба каталогов позволяет найти любой объект по одному из его атрибутов.

Служба каталогов Active Directory может быть установлена на серверах, работающих под управлением операционных систем Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition. Она хранит сведения об объектах сети и упрощает поиск и использование этих сведений пользователям и администраторами. В Active Directory основой для логической, иерархической организации сведений каталога служит структурированное хранилище данных. Это хранилище данных, называемое так же каталогом, содержит сведения об объектах Active Directory. В число этих объектов обычно входят общие ресурсы, такие как серверы, тома, принтеры, а также учетные записи сетевых пользователей и компьютеров.

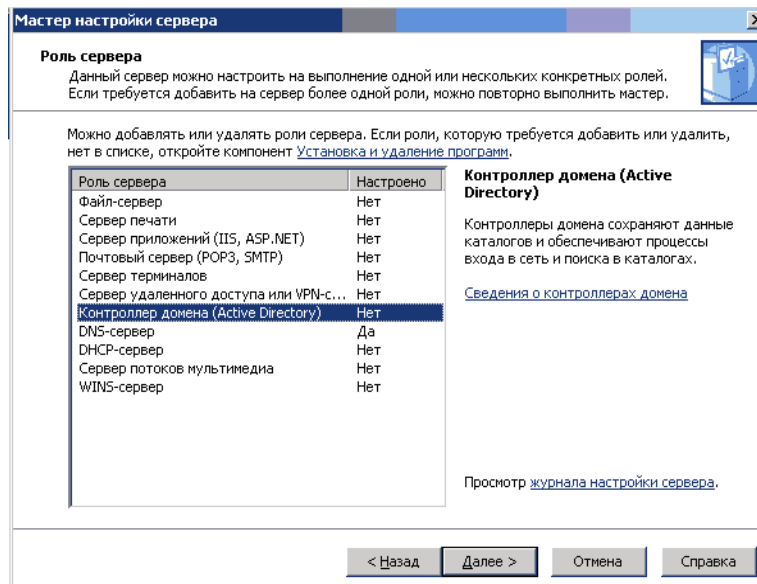
В Windows Server 2003 Active Directory может быть интегрирована с DNS воедино. DNS представляет собой распределенное пространство имен, которое используется в Интернет и в котором именам отдельных компьютеров и служб ставятся в соответствие адреса, формируемые по правилам протокола TCP/IP. При создании контроллера домена, то есть сервера, управляющего работой Active Directory, мастер предлагает создать и настроить DNS-сервер. В этом случае запускается DNS-сервер и создается зона (контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление), одноименная с доменом.

Контроллеры домена хранят данные и управляют взаимодействием пользователей с доменом, включая процесс входа в домен, проверку подлинности и поиск в каталогах. Чтобы предоставить сетевым пользователям и компьютерам службу каталогов Active Directory, нужно настроить данный сервер как контроллер домена.

Для настройки сервера в качестве контроллера домена необходимо установить на данный сервер Active Directory. В мастере установки Active Directory доступны четыре параметра: можно создать дополнительный контроллер домена в существующем домене, контроллер домена для нового дочернего домена, контроллер домена для нового доменного дерева или новый контроллер домена для нового леса. Рассмотрим создание контроллера домена для нового леса.

Операционная система Windows Server 2003 позволяет настроить данный сервер как контроллер домена. Для этого нам необходимо выполнить следующие действия: открыть оснастку "Управление данным сервером"; выбрать ссылку "Добавить или удалить роль"; на странице "Предварительные шаги" прочитать информацию о сетевых соединениях и подтвердить, что все они доступны; на странице "Параметры настройки" выбрать вариант "Особая конфигурация".

На экран будет выведена новая страница, представленная на рис. 20 - Роль сервера.



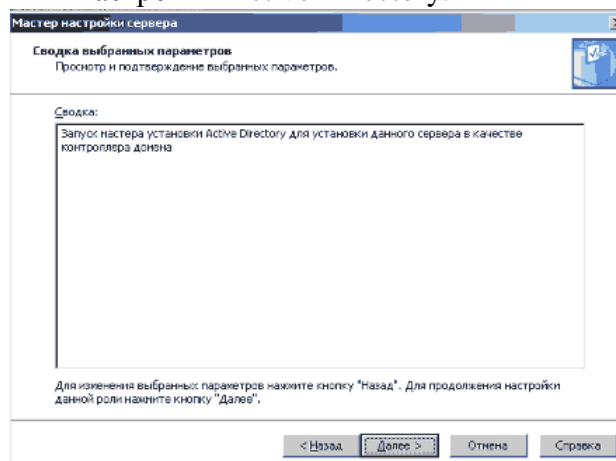
Роль сервера

На этой странице мы выбираем из приведённого списка "Контроллер домена (Active Directory)" и нажимаем кнопку "Далее".

Появится страница "Сводка выбранных параметров" (рис. 21), в которой можно просмотреть и подтвердить выбранные параметры:

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее".

Появится страница "Применение выбранных параметров", которая будет находиться на экране всё время до окончания установки и настройки Active Directory.

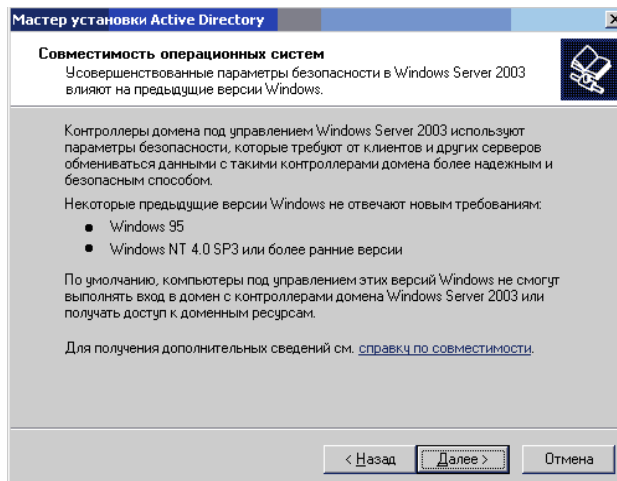


Сводка выбранных параметров

Автоматически запустится мастер установки Active Directory.

Нажимаем кнопку "Далее" для продолжения. К этой странице можно вернуться из любого места мастера, пока не нажата кнопка "Готово" на последней странице.

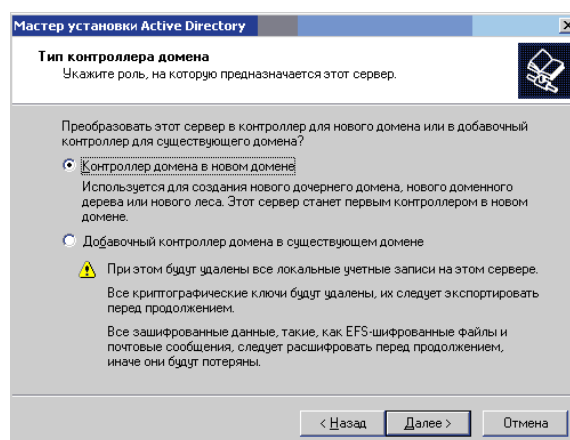
Мастер установки выведет на экран страницу, представленную на рис, "Совместимость операционных систем", в которой приводится информация о влиянии усовершенствованных параметров безопасности в Windows Server 2003 на совместимость с предыдущими версиями Windows.



Совместимость операционных систем

Прочитав сведения, приведённые на этой странице, нажимаем кнопку "Далее".

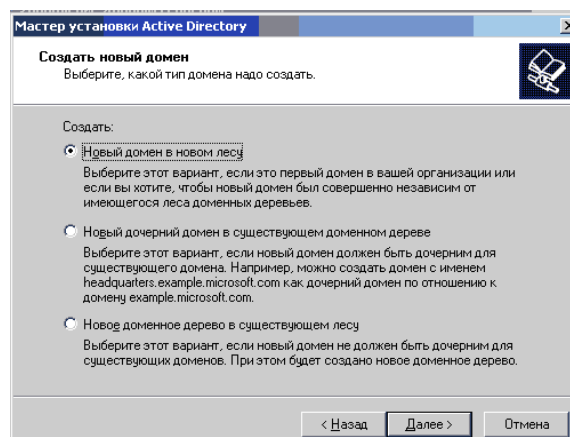
На странице "Тип контроллера домена" выбираем вариант "Контроллер домена в новом домене"



Тип контроллера домена

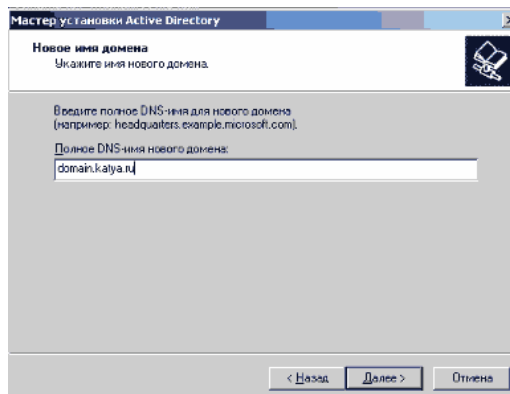
Для продолжения нажимаем кнопку "Далее".

На появившейся странице, представленной на рис. "Создать новый домен" выбираем вариант "Новый домен в новом лесу".



Тип контроллера домена

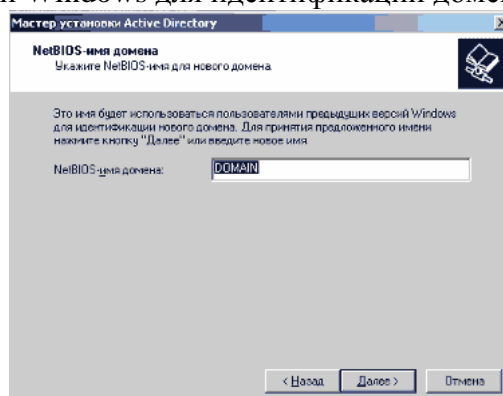
Для продолжения нажимаем кнопку "Далее". На странице "Новое имя домена" (рис. 26) вводим полное DNS-имя нового домена.



Новое имя домена

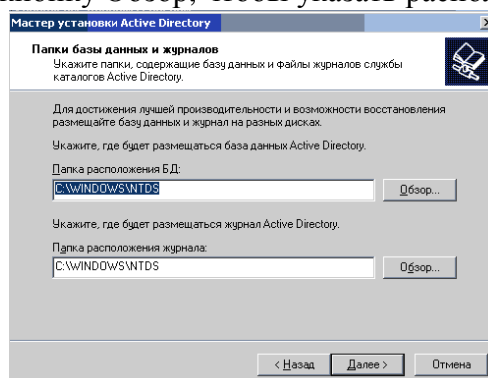
Полное DNS-имя также называют полным доменным именем (FQDN). Домены Active Directory обозначаются с помощью DNS-имен и повторяют иерархическую структуру DNS. DNS-имена для леса Active Directory должны начинаться с зарегистрированного суффикса домена DNS, который зарезервирован организацией для использования в Интернете, например microsoft.com. Для продолжения нажимаем кнопку "Далее".

На странице NetBIOS-имя домена проверяем NetBIOS-имя, которое будет использоваться пользователями предыдущих версий Windows для идентификации домена (рис. 27).



NetBIOS-имя домена

Домены Active Directory обозначаются в соответствии со стандартами именования DNS, однако при создании доменов Active Directory необходимо задать также NetBIOS-имя. NetBIOS-имена по возможности должны совпадать с первой меткой DNS-имени домена. Если первая метка DNS-имени домена Active Directory отличается от его NetBIOS-имени, в качестве полного доменного имени используется DNS-имя, а не NetBIOS-имя. Например, если первая метка полного DNS-имени домена - child (child.microsoft.com), а NetBIOS-имя домена - sales, полным доменным именем будет child.microsoft.com. Для продолжения нажимаем кнопку "Далее". На странице "Папки базы данных и журналов", представленной на рис., вводим расположение, в которое нужно установить папки базы данных и журналов (или нажимаем кнопку Обзор, чтобы указать расположение).

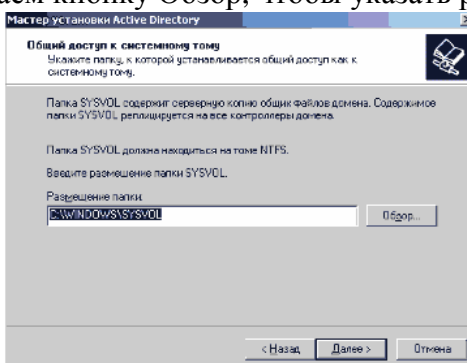


Папки базы данных и журналов

При этом нужно убедиться, что на диске достаточно места для размещения базы данных каталога и файлов журналов, чтобы избежать проблем при установке или удалении Active Directory. Мастеру установки Active Directory необходимо 250 МБ дискового пространства для установки базы

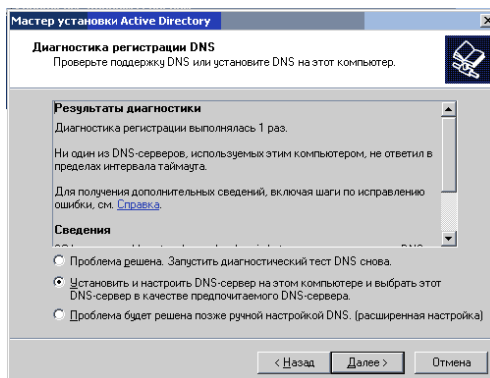
данных Active Directory и 50 МБ для файлов журналов. Рекомендуется размещать данные файлы в разделе NTFS. Для продолжения нажимаем кнопку "Далее".

На странице "Общий доступ к системному тому" указываем расположение, в которое следует установить папку Sysvol (или нажимаем кнопку Обзор, чтобы указать расположение).



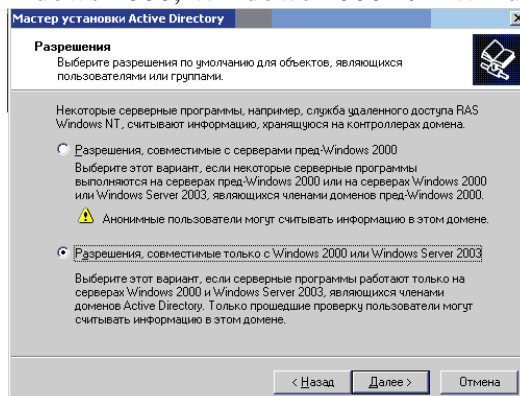
Общий доступ к системному тому

Папка Sysvol должна находиться в томе NTFS, так как в ней находятся файлы, реплицируемые между контроллерами домена в домене или лесу. Эти файлы содержат сценарии, системные политики для Windows NT 4.0 и более ранних версий, общие папки NETLOGON и SYSVOL и параметры групповой политики. Для продолжения нажимаем кнопку "Далее". На странице "Диагностика регистрации DNS" (рис. 30) проверяем правильность установки параметров. Если в окне "Результаты диагностики" отображается сообщение об ошибках диагностики, можно нажать кнопку "Справка" для получения дополнительных инструкций по устранению ошибки. Для продолжения нажимаем кнопку "Далее".



Диагностика регистрации DNS

На странице "Разрешения" выбираем требуемый уровень совместимости приложений с операционными системами пред-Windows 2000, Windows 2000 или Windows Server 2003.



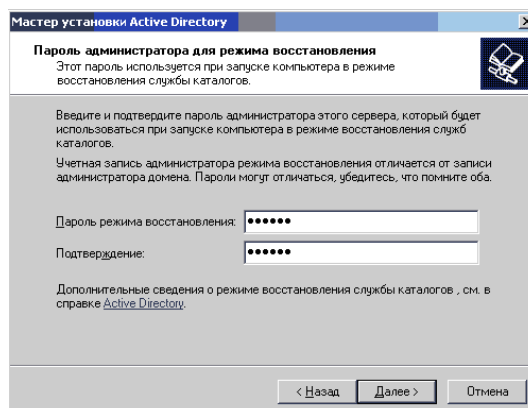
Выбор требуемого уровня совместимости

На серверах под управлением Windows NT 4.0 и более ранних версий доступ на чтение сведений о пользователях и группах открыт для анонимных пользователей, так что существующие приложения, в том числе Microsoft BackOffice, SQL Server и некоторые приложения других производителей, работают правильно. В Windows 2000 и системах семейства Windows Server 2003 члены группы "Анонимный вход" имеют доступ на чтение к этим сведениям, только если они включены в группу "Пред-Windows 2000 доступ". Для того чтобы добавить группы "Анонимный

вход" и "Все" в группу "Пред-Windows 2000 доступ" нужно выбрать вариант "Разрешения, совместимые с серверами пред-Windows 2000". Для того чтобы запретить доступ на чтение сведений о пользователях и группах членам группы "Анонимный вход" мы выбираем вариант "Разрешения, совместимые только с серверами Windows 2000 или Windows Server 2003".

После выбора одного из вариантов можно вручную переключаться между обратной совместимостью и высоким уровнем безопасности объектов Active Directory. Для этого нужно открыть компонент "Active Directory - пользователи и компьютеры" и добавить группу безопасности "Анонимный вход" в группу безопасности "Пред-Windows 2000 доступ". Для продолжения нажимаем кнопку "Далее".

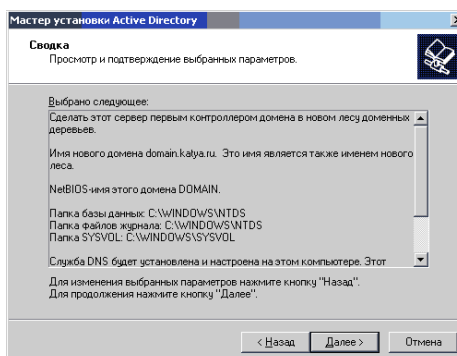
На странице "Пароль администратора для режима восстановления" нужно ввести и подтвердить пароль для учетной записи администратора режима восстановления для данного сервера.



Пароль администратора для режима восстановления

В качестве паролей режима восстановления каталогов необходимо использовать надежные пароли. Этот пароль необходимо знать для восстановления резервной копии состояния системы данного контроллера домена. Данный пароль нужно также использовать при запуске контроллера домена в режиме восстановления служб каталогов. Для продолжения нажимаем кнопку "Далее".

После этого просматриваем сведения на странице "Сводка", представленной на рис., и нажимаем кнопку "Далее".



Просмотр и подтверждения выбранных параметров

Мастер установки настроит Active Directory: После завершения установки нажимаем кнопку "Готово". Для перезагрузки компьютера нажимаем кнопку "Перезагрузить сейчас", чтобы изменения вступили в силу.

После перезагрузки сервера "Мастер настройки сервера" отобразит страницу "Этот сервер теперь является контроллером домена"

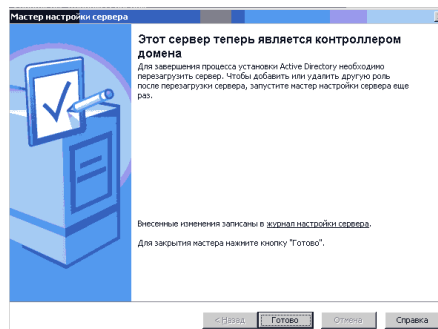


Рис. 34. Подтверждение контроллера домена

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 24

ПАРАМЕТРЫ ОБЩЕГО ДОСТУПА

Цель работы: научиться настраивать общие папки, для организации общего доступа к файлам и папкам для компьютеров, которые расположены в одной локальной группе или в одном домене.

Задачи работы:

Оснащение: МУ к ПЗ

Порядок выполнения работы

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

При работе с домашней локальной сетью или с компьютерами интрасети организации вам придется настраивать общие папки, так как, вероятнее всего, что ваши пользователи захотят разрешать сотрудникам просматривать, изменять и создавать файлы и папки для компьютеров, которые расположены в одной локальной группе или в одном домене. В настройке общего доступа к файлам и папкам нет ничего сложного, но в связи с тем, что для открытия общего доступа нужны права администратора, не всем пользователям вашей сети будет предоставлена такая возможность. Но после того как вы настроите на пользовательских компьютерах параметры общего доступа, пользователи смогут самостоятельно предоставлять доступ к своим папкам и файлам.

Какие же задачи можно выполнить при помощи общего доступа? Для того чтобы ваши пользователи могли просматривать содержимое локальной сети и иметь доступ к компьютерам и

устройствам вы можете включить сетевое обнаружение. Если к каждому компьютеру вашей сети не подключен локальный принтер, вам придется открывать общий доступ к принтерам, для того чтобы пользователи могли распечатывать свою документацию. Вы можете предоставлять общий доступ к ресурсам компьютера, как для всех пользователей, так и для тех пользователей, учетные данные которых имеются на компьютере, предоставляющем общий доступ к файлам и папкам. Вы можете разрешить пользователям обмениваться музыкой, видеофайлами и картинками, разрешив общий доступ к потоковому мультимедиа и прочее.

Общий доступ к файлам и принтерам

Если ваш компьютер находится в локальной сети, то, возможно, вы захотите предоставить некоторые файлы или папки для общего просмотра, а также дать возможность использовать ваш принтер остальным членам локальной сети. Если вы хотите, чтобы другие пользователи могли просматривать и выполнять какие-либо действия с файлами, для которых вы предоставляете общий доступ, необходимо включить данный функционал. По умолчанию, для профиля «**Домашний или рабочий**» данная возможность включена, а для профиля «**Общий**» - отключена. Для того чтобы включить или отключить данную функцию и добавить файлы в общедоступную папку, выполните следующие действия:

1. Откройте окно «**Дополнительные параметры общего доступа**»;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например «**Домашний или рабочий**»;
3. В группе «**Общий доступ к файлам и принтерам**» выберите параметр «**Включить общий доступ к файлам и принтерам**» и нажмите на кнопку «**Сохранить изменения**»;
4. По умолчанию, общий доступ к файлам или папкам можно предоставлять, скопировав или переместив их в папку «**Общие**», которая находится в %USERS%\Public (%Пользователи%\Общие).

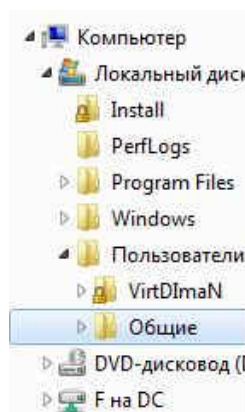


Рис. 3.2. Папка «Общие»

Доступ к общим папкам

Как было указано выше, наряду с папками пользовательских учетных записей, операционная система Windows создает папку «**Общие**», общий доступ для которой открыт по умолчанию для профиля «**Домашний и рабочий**». При помощи окна «**Дополнительные параметры общего доступа**» вы можете запретить доступ к данной папке. Для этого выполните следующие действия:

1. Откройте окно «**Дополнительные параметры общего доступа**»;
2. Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например «**Домашний или рабочий**»;
3. В группе «**Доступ к общим папкам**» выберите опцию «**Отключить общий доступ**».

Следует учесть, что у пользователей, которые уже успели подключиться к данной папке, все еще будет доступ для использования ресурсов, которые в ней расположены.

Потоковая передача мультимедиа

При помощи параметров потоковой передачи мультимедиа для компьютеров и устройств, вы можете устанавливать разрешения для папок с музыкой, видео файлами и изображениями, которые

будут доступны для передачи в потоковом режиме на устройства и компьютеры в сети в «Пригрывателе Windows Media». Для настройки данных параметров вам нужно перейти по ссылке «Выберите параметры потоковой передачи мультимедиа» в группе «Потоковая передача мультимедиа» окна «Дополнительные параметры общего доступа».

Подключение общего доступа к файлам

При помощи параметров, расположенных в данной группе, вы можете указать тип шифрования для защиты подключения общего доступа. Шифрование применяется для обеспечения защиты файлов и папок, предоставленных для общего доступа. Операционная система Windows 7 предоставляет два алгоритма для шифрования подключений:

- 40-битное или 56-битное шифрование – DES (Data Encryption Standard). Это симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных. DES разработан фирмой IBM и утвержден правительством США в 1977 году как официальный стандарт;
- 128-битное шифрование – Advanced Encryption Standard (AES). Это также симметричный алгоритм блочного шифрования (размер блока 128 бит, ключ 128/192/256 бит), принятый в качестве стандарта шифрования правительством США по результатам конкурса AES. Этот алгоритм хорошо проанализирован и сейчас широко используется, как это было с его предшественником DES.

Значение по умолчанию для всех профилей – 128-битное шифрование для защиты подключений общего доступа.

Общий доступ с парольной защитой

В целях безопасности, по умолчанию доступ к общим папкам защищен паролем. Для получения доступа к пользовательским общим папкам и файлам на другом компьютере необходимо ввести соответствующие данные своей учетной записи. Этот метод используется для разрешения доступа лишь к указанному набору ресурсов.

Метод предоставления доступа к файлам и папкам обычно используется в том случае, если одним пользователям разрешен доступ к одному набору общих ресурсов, а другим открыт полный доступ. Для того чтобы отключить доступ с парольной защитой (что в принципе на предприятиях делать крайне не желательно), выполните следующие действия:

- 1 Откройте окно «Дополнительные параметры общего доступа»;
- 2 Разверните сетевой профиль, для которого будет открыт общий доступ к файлам и принтерам, например «Домашний или рабочий»;
- 3 В группе «Общий доступ с парольной защитой» выберите опцию «Отключить общий доступ с парольной защитой» и нажмите на кнопку «Сохранить изменения».

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ САМОПОДГОТОВКИ

1. Каким образом можно получить доступ к окну «Дополнительные параметры общего доступа»?
2. Опишите функции «Сетевого обнаружения».
3. Какие особенности функционала сетевого обнаружения существуют в доменном окружении?
4. В каком случае доступ к файлам и папкам можно организовать по умолчанию?
5. Приведите примеры различных видов доступа для различных пользователей.
6. Что представляют собой дополнительные настройки для папок открытого доступа?
7. Опишите ситуацию подключения к общим папкам пользователей компьютеров сети.
8. Для чего и каким образом настраивается потоковая передача мультимедиа?
9. Опишите алгоритмы шифрования для подключений, которые предоставляет операционная система Windows 7 .
10. В каких ситуациях целесообразно назначать доступ с парольной защитой, и какие особенности настройки при этом возникают?

Каким образом настраивается доступ к файлам и папкам для домашней группы?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 25
Управление общими папками

Цель работы: научиться настраивать доступ к папкам.

Оснащение: МУ к ПЗ

Порядок выполнения работы

ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Как в домашних условиях, так и в корпоративной среде, на ваших компьютерах может быть предоставлен общий доступ к десяткам папок. Назначив для каждой папки специфические разрешения, вскоре вы можете запутаться в предоставленных правах для своих папок. Целесообразнее управлять общими папками на компьютере при помощи оснастки консоли управления Microsoft «**Общие папки**». Именно при помощи оснастки «**Общие папки**», вы можете создавать общие ресурсы, а также устанавливать всевозможные разрешения для таких ресурсов. Помимо этого, вам предоставляется возможность просматривать и отключать открытые файлы и сеансы пользователей, подключенных к вашим общим ресурсам. Также вы можете настраивать доступ к своим папкам в автономном режиме, управлять ограничением числа пользователей, которые могут одновременно получить доступ к вашим ресурсам и многое другое. В этой лабораторной работе вы узнаете не только об интерфейсе оснастки «**Общие папки**», но и выполнении аналогичных действий средствами командной строки при помощи команд net share, net files и net session.

КОНТРОЛЬНЫЕ ВОПРОСЫ И ЗАДАНИЯ ДЛЯ САМОПОДГОТОВКИ

1. Для чего предназначена оснастка «**Общие папки**», и каким образом можно получить к ней доступ?
2. Что позволяет сделать утилита командной строки **NET SHARE**, и какой формат команды для нее используется?
3. Используя утилиту командной строки **NET SHARE**, продемонстрируйте ситуации создания общего ресурса и прекращения доступа к ресурсу.
4. Какие параметры разрешения доступны общих ресурсов?
5. Что обеспечивает функционал BranchCache, и каким образом он настраивается через диалоговые окна и командную строку?
6. Каким образом с помощью оснастки «**Общие папки**» и через командную строку закрыть открытые файлы?
7. Каким образом можно управлять сеансами?

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 26

Настройка общего доступа к принтеру

Цель: научиться настраивать общий доступ к принтеру

Оснащение: МУ к ПЗ

Порядок выполнения работы

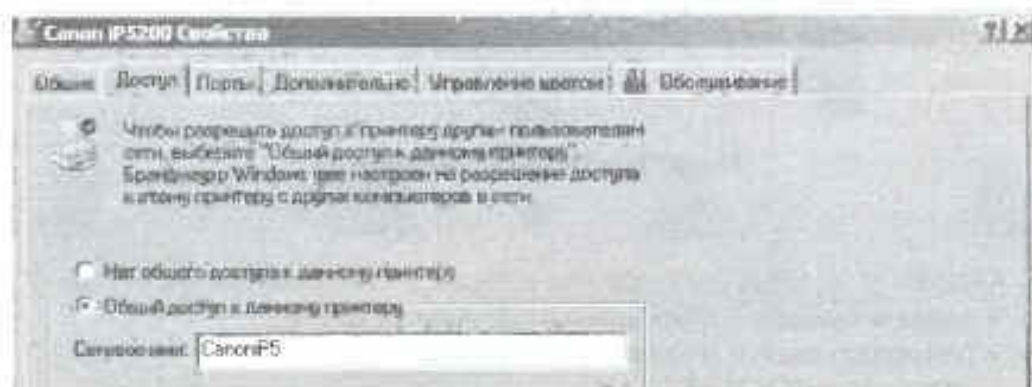
Задание. В локальной сети, на компьютерах которой установлена операционная система Windows, предоставить общий доступ к принтеру.

Варианты выполнения работы:

- предоставление общего доступа к принтеру в **локальной сети** компьютерного класса;
- предоставление общего доступа к принтеру в домашней локальной сети. (В данной работе используется домашняя локальная сеть в составе настольного компьютера Celeron, к которому подключен принтер, и **ноутбука Bliss**.)

Предоставление общего доступа к принтеру в домашней локальной сети на компьютере, к которому подключен принтер, установим общий доступ к принтеру.

1. В операционной системе Windows ввести команду [*Настройка-Принтеры и факсы-Принтер*]. В контекстном меню принтера выбрать пункт *Свойства*. В появившемся диалоговом окне выбрать вкладку *Доступ* и на ней установить переключатель в положение *Общий доступ к данному принтеру*. На каждом компьютере, подключенном к локальной сети с помощью *Мастера настройки сети*, зададим описание и имя каждого **компьютера**, имя общей рабочей группы и включим общий доступ к файлам и принтерам.

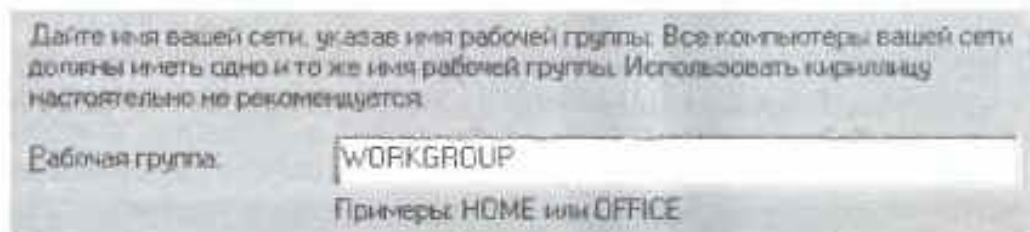


2. Ввести команду [*Настройка Панель у правления - Мастер настройки сети*].

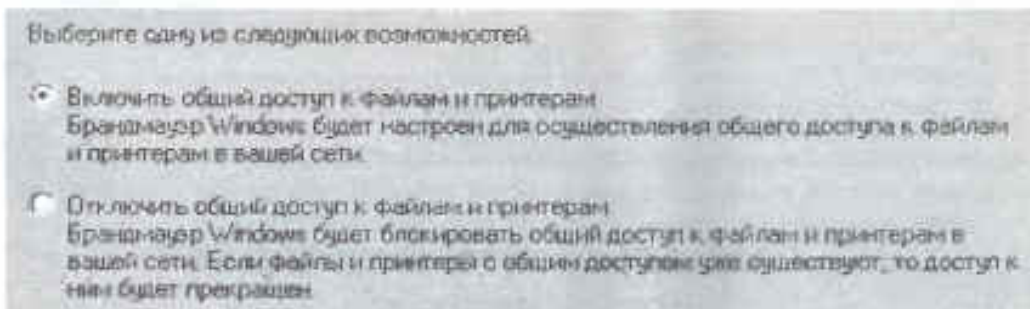
3. В одном из диалоговых окон *Мастера* дать описание и имя каждого компьютера.



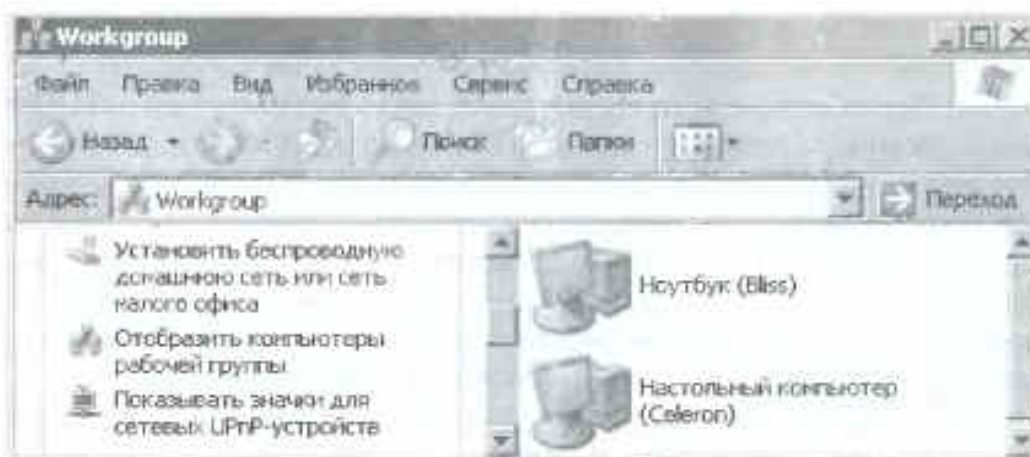
4. На всех **компьютерах** локальной сети задать одно имя общей рабочей группы.



5. На всех компьютерах локальной сети включить общий доступ к файлам и принтерам. На каждом компьютере локальной сети посмотрим перечень компьютеров, входящих в выбранную рабочую группу локальной сети.



6. На *Рабочем столе* щелкнуть по значку **Сетевое окружение** и в открывшемся диалоговом окне щелкнуть по ссылке *Отобразить компьютеры рабочей группы*. Через некоторое время появится перечень компьютеров, входящих в заданную рабочую группу. На каждом компьютере, входящем в выбранную рабочую группу локальной сети, убедимся, что принтер доступен для печати документов.



7. Щелкнуть по значку компьютера, к которому подключен принтер. В диалоговом окне должен отображаться значок принтера.



Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 27

Подключение к домену

Цель работы: научиться создавать учетные записи компьютеров при помощи консоли *Active Directory* — *пользователи и компьютеры* (Active Directory Users and Computers) и команды DSADD; научиться присоединять компьютер к домену.

Оснащение: МУ к ПЗ

Порядок выполнения работы

Упражнение 1. Создание объектов компьютеров в консоли *Active Directory* — *пользователи и компьютеры*

1. Откройте консоль *Active Directory* — *пользователи и компьютеры*.
2. В ОП Servers создайте объект для компьютера с именем SERVER02. Задайте только имя компьютера. Не меняйте значения других параметров по умолчанию. Заметьте, что у компьютера, как и у пользователя, два имени — указанное имя компьютера и имя в формате пред-
Windows 2000. На практике лучше, чтобы эти имена оставались одинаковыми.

Упражнение 2. Создание учетных записей компьютеров командой DSADO

Из командной строки выполните следующую команду:

```
dsadd computer ?cn=desktop03,ou=servers,dc=contoso,dc=com?
```

Упражнение 3. Перемещение объекта компьютера

1. Откройте консоль *Active Directory* — *пользователи и компьютеры*.
2. Командой **Переместить (Move)** переместите компьютер Desktop03 из ОП Servers в ОП Desktops.
3. Перетащите значок Server02 из контейнера Servers в Computers.
4. Выберите контейнер Computers и убедитесь, что Server02 появился в нужном месте. При перетаскивании объектов можно ошибиться.

5. Откройте окно свойств для контейнера Computers. Вы увидите, что здесь нет вкладки **Групповая политика (Group Policy)**, в отличие от ОП, например Servers. Это одна из причин, почему принято создавать одно или несколько дополнительных ОП для объектов компьютеров.

6. Из командной строки выполните следующую команду:

```
dsmove ?CN=Server02,CN=Computers,DC=contoso,DC=com? -newparent ?OU=Servers,DOcontoso,DC=com?
```

Эта команда, как легко догадаться, перемещает объект компьютера обратно в ОП Servers.

7. Проверьте, что этот компьютер снова находится в ОП Servers.

Упражнение 4 (необязательное). Присоединение компьютера к домену

Для этого упражнения необходим второй компьютер, подключенный к Server01. Кроме того, нужно правильно сконфигурировать DNS, чтобы для Server01 была создана запись ресурса службы (SRV). На втором компьютере DNS должна быть сконфигурирована так, чтобы он мог находить Server01 как контроллер домена contoso.com.

1. Если у вас есть второй компьютер, который можно в следующем упражнении присоединить к вашему домену, создайте для него учетную запись в ОП Desktops при помощи консоли *Active Directory* — *пользователи и компьютеры* (Active Directory Users And Computers) или команды DSADD. Убедитесь, что используемое вами имя совпадает с именем этого компьютера.

2. Войдите в систему на этом компьютере. Чтобы изменять членство этого компьютера в доменах, нужно войти в систему под учетной записью локальной группы *Администраторы* (Administrators).

3. Откройте вкладку **Имя компьютера (Computer Name)**. Для этого дважды щелкните **Система (System)** в *Панели управления* или в папке **Сетевые подключения (Network Connections)**, в меню **Дополнительно (Advanced)** выберите **Сетевая идентификация (Network Identification)**.

4. Щелкните **Изменить (Change)**.
5. Установите переключатель в положение **домена (Domain)** и введите DNS-имя домена: contoso.com.
6. Щелкните **ОК**.
7. По запросу введите имя и пароль учетной записи администратора домена contoso.com.

8. Щелкните **ОК**.

9. Вам будет предложено перезагрузить систему. Щелкайте **ОК** в ответ на все сообщения и закройте все диалоговые окна. Перезагрузите систему.

Контрольные вопросы

Что такое домен

Что такое актив директорий

Список используемой литературы

С. Бигелец Устройство и ремонт персонального компьютера 2018г.

Преподаватель

Н.А Мельникова

Практическое занятие 28

Настройка сетевых протоколов

Цель: знать виды и классификацию локальных сетей, физические среды передачи данных, научиться устанавливать и настраивать сетевой интерфейс

Оборудование: IBM-PC совместимый компьютер, сетевая карта.

Программное обеспечение: MS Windows'

Перед началом настройки сетевого интерфейса необходимо установить и настроить сетевую карту. После корректной установки драйвера сетевой карты необходимо настроить сетевые протоколы, которые будут использоваться на данном интерфейсе. После настройки протоколов проверяется работа системы в сети, начиная с команд ping для проверки связности на физическом и канальном уровне, tracert для проверки работы маршрутизации, и заканчивая работой конкретных приложений (электронная почта, веб-сервер) прикладном уровне.

Порядок выполнения:

Подготовка к выполнению работы

1. Изучите настоящие указания, уточните непонятные моменты.
2. Если монитор вычислительной системы имеет питание, отдельное от системного блока, включите монитор.
3. Включите компьютерную систему выключателем системного блока.
4. При появлении запроса о пароле нажмите на клавиатуре клавишу **Esc**.
5. **Установка протоколов**
6. Нажмите кнопку **Пуск** на панели задач. Выберите пункт **Настройка -> Панель**

Управления.

7. Нажмите кнопку **Добавить:** Выберите тип устанавливаемого компонента: Протокол. Нажмите кнопку **Добавить:**
8. Выберите соответствующие пункты в окнах Изготовители: Microsoft и Сетевые протоколы: IPX/SPX-совместимый протокол. Нажмите кнопку **ОК**.
9. Нажмите кнопку **ОК**.
10. Для корректной настройки драйвера перезагрузите систему (**условно**).
11. **Удаление протоколов**
12. Нажмите кнопку **Пуск** на панели задач. Выберите пункт **Настройка -> Панель**

Управления.

13. Откройте объект **Сеть**. В появившемся окне на вкладке **Конфигурация** выберите компонент IPX/SPX-совместимый протокол. Нажмите кнопку **Удалить:**
14. Для корректной настройки драйвера перезагрузите систему (**условно**).
15. **Настройка сетевого протокола TCP/IP**
16. Выберите компонент **TCP/IP**. Нажмите кнопку **Свойства**. В появившемся окне:
 - на вкладке **Адрес IP** снимите значения параметров IP-адрес и Маска подсети
 - на вкладке **Шлюз** снимите значения параметра Установленные шлюзы
 - на вкладке **Конфигурация** снимите значения параметров Имя компьютера, Домен,

Порядок просмотра серверов DNS.

- Нажмите кнопку **ОК**.

Проверка настройки протокола

17. После перезагрузки компьютера проверьте работу сетевого интерфейса командой ping IP-адрес и работу сервера DNS командой ping доменное_имя. Адреса и доменные имена для проверки работы сети (*получить у преподавателя*):

18.

IP-адрес	Доменное имя	Примечание

--	--	--

19. Проверьте работу маршрутизации командой tracert IP-адрес (tracert доменное_имя).
Адреса и доменные имена для проверки работы сети (получить у преподавателя).

20. Заполните таблицу:

№ п/п	Наименование	Значение
1.	Сетевая плата	
2.	Используемые протоколы	
3.	IP-адрес	
4.	Маска подсети	
5.	Доменное имя компьютера	
6.	DNS-сервер(ы)	
7.	Шлюз	

Завершение работы

20. Уточните у преподавателя порядок завершения работы с компьютером. Приведите компьютер в исходное состояние.

Вопросы к защите:

1. Порядок настройки стека протоколов TCP/IP.
2. Что такое: IP-адрес, маска подсети, доменное имя, DNS-сервер, шлюз.
3. Маршрутизация. Принципы маршрутизации.
4. Назначение и принцип работы сервиса ARP.
5. Как определить доступность вычислительной системы по сети?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 29

Настройка контроллера домена и DNS-сервера

Цель работы: приобретение студентами практических навыков установки и настройки роли DNS.

Оснащение: МУ к ПЗ, ПК

Порядок выполнения работы

Протокол, определявший порядок обмена информацией в Интернете, описывал, в том числе и систему адресации компьютеров, объединенных в эту сеть. Согласно этой системе, каждому компьютеру присваивался уникальный четырехбайтовый адрес, который стали называть IP-адрес. Стандарт нового протокола и, соответственно, системы адресования были приняты в 1982 году. Однако человеку гораздо проще запомнить некоторое слово, чем четыре бессодержательных для него числа. Из-за этого сразу после начала работы новой сети у пользователей стали появляться списки, в которых хранились не только адреса, но и соответствующие им имена узлов. Эти данные, обычно хранившиеся в файле с именем `hosts`, позволяли при указании имени узла мгновенно получить его IP-адрес. Позже процесс внесения корректуры в эти файлы был усовершенствован - последнюю версию файла `hosts` можно было скачать с нескольких серверов с заранее определенными адресами. С ростом числа компьютеров в сети корректировать эти файлы вручную стало невозможно. Появилась необходимость в глобальной базе имен, позволяющей производить преобразование имен в IP-адреса без хранения списка соответствия на каждом компьютере. Такой базой стала DNS (Domain Name System) - система именования доменов, которая начала работу в 1987 году.

В Интернете существует множество DNS-серверов, предоставляющих клиентам необходимую информацию об именах узлов сети. Важнейшим качеством DNS является порядок их работы, позволяющий DNS-серверам синхронно обновлять свои базы. Добавление адреса нового сайта в Интернете проходит за считанные часы.

Вторая особенность системы - это организация DNS-серверов в виде иерархической структуры. Например, запрос от клиента об имени `ftp.microsoft.com` может пройти через несколько DNS-серверов, от глобального, содержащего информацию о доменах верхнего уровня (`.com`, `.org`, `.net` и т. п.), до конкретного сервера компании Microsoft, в чьих списках перечислены поддомены вида `*.microsoft.com`, в числе которых мы и находим нужный нам `ftp.microsoft.com`. При этом множество DNS-серверов организуется в зоны, имеющие права и разрешения, делегированные вышестоящим сервером. Таким образом, при добавлении нового поддомена на местном сервере уведомления остальных серверов в Глобальной сети не производятся, но информация о новых серверах оказывается доступной по запросу.

Проследим прохождение запроса. При установке (точнее, при настройке) клиенту указывается как минимум один DNS-сервер (как правило, их два) - его адрес выдается провайдером. Клиент посылает запрос этому серверу. Сервер, получив запрос, либо отвечает (если ответ ему известен), либо пересылает запрос на "вышестоящий" сервер (если он известен) или на корневой (каждому DNS-серверу известны адреса корневых DNS-серверов). Так выглядит "восходящая иерархия". Затем запрос начинает спускаться вниз - корневой сервер пересылает запрос серверу первого уровня, тот - серверу второго уровня и т.д.

Помимо "вертикальных связей", у серверов есть еще и "горизонтальные" отношения - "первичный - вторичный". Действительно, если предположить, что сервер, обслуживающий какой-то домен и работающий "без страховки" вдруг перестанет быть доступным, то все машины, расположенные в этом домене, окажутся недоступны. Именно поэтому при регистрации домена второго уровня выдвигается требование указать минимум два сервера DNS, которые будут этот домен обслуживать.

Полезным свойством DNS является умение использовать "пересыльщиков" (`forwarders`). "Честный" DNS-сервер самостоятельно опрашивает другие сервера и находит нужный ответ, но если ваша сеть подключена к Интернету по медленной (например, `dial-up`) линии, то этот процесс может занимать довольно много времени. Вместо этого можно перенаправлять все запросы, скажем, на сервер провайдера, а затем принимать его ответ. Использование "пересыльщиков" может оказаться интересным и для больших компаний с несколькими сетями: в каждой сети можно поставить относительно слабый DNS-сервер, указав в качестве "пересыльщика" более мощную машину,

подключенную по быстрой линии. При этом все ответы будут кэшироваться на этом мощном сервере, что ускорит разрешение имен для целой сети.

С ростом числа доменных имен работа между серверами была распределена по принципу единоначалия. Идея проста. Если организация владеет собственным доменным именем (например, microsoft.com или white-house, gov), то именование внутри своего домена она производит самостоятельно. Единственная сложность при такой работе - предоставление вышестоящими серверами этих прав нижестоящим серверам.

Уточним термины. Домен - это некий контейнер, в котором могут содержаться хосты и другие домены. Имя домена может не совпадать с именем контроллера домена, то есть домен - это виртуальная структура, не привязанная к компьютеру. Хост же, напротив, соответствует физическому компьютеру, подключенному к сети. Имя хоста является именем конкретного компьютера. Имя хоста может совпадать с именем домена. Имя домена может совпадать с именем зоны, к которой он принадлежит, в этом случае домен является корневым в зоне. При этом зона не обязана содержать в себе одноименный (корневой) домен.

Зона - это контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление, то есть зоны являются контейнерами для доменов и хостов. Зоны могут быть вложены одна в другую. Разница между зонами и доменами в том, что домену может принадлежать несколько зон, содержащих различные его поддомены. Это дает возможность делегировать полномочия для поддоменов и управлять группами поддоменов.

Зоны используются для делегирования полномочий. Каждый домен должен находиться в составе зоны при создании поддомена последний может быть переведен в новую зону, либо оставлен в зоне стоящего над ним домена. Для каждой зоны разрешения на создание или удаление всех входящих в нее доменов делегируются отдельно. Для нормальной работы корпоративной сети в большинстве случаев хватает единственной зоны, более того, очень часто системные администраторы ограничиваются созданием единственного домена.

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 30 Настройка DHCP- сервера

Цель: научиться настраивать DHCP-сервер

Оснащение: МУ к ПЗ, ПК

Порядок выполнения работы

1. Проверьте установлен ли на узлах host1 и host2 пакет dhcp, на узлах host2 и host3 пакет dhclient. Если нет, то установите его.
2. Используя файлы описания настроек сетевых интерфейсов (ifcfg-*) и скрипт /etc/init.d/network, сконфигурируйте внешний интерфейс узла host3 так, чтобы он автоматически получал настройки. Определите какие настройки он получил?
3. Изучите файл /var/lib/dhcp/dhclient-eth0.leases. Опишите полученную аренду сетевых настроек. Кто их выдал?
4. На узле host1.
 1. Изучите пример конфигурационного файла dhcpd.conf (/usr/share/doc/dhcp-*/dhcpd.conf.sample).
 2. Разработайте свой файл конфигурации (/etc/dhcpd.conf) таким образом, чтобы сервер предлагал адреса из сети 172.16.N.0/24. Параметры области следующие:
 - адреса выдаются из диапазона от 120 до 140;
 - шлюз - 172.16.N.1;
 - DNS сервер 172.16.N.1;
 - имя домена задайте согласно заданию.
 3. Запустите сервер dhcpd (/etc/init.d/dhcpd start). При помощи утилиты netstat проверьте, что сервер готов принимать запросы по протоколу UDP и порту 67. Посмотрите сообщения, произведённые DHCP сервером в системном журнале (/var/log/messages).
 4. Сконфигурируйте сервис dhcpd так, чтобы он автоматически запускался при загрузке системы на уровнях 3 и 5.
 5. Настройте внутренние интерфейсы узлов host2 и host3 на автоматическое получение параметров. Проверьте правильность работы dhcp сервера. Убедитесь, что клиенты получили адреса в аренду (проверьте содержимое каталога /var/lib/dhcp).
 6. Задайте на DHCP сервере резервирование для узла host3. Параметры резервирования следующие:
 - имя узла - host3.groupN.local
 - шлюз по умолчанию - host2На host3 переполучите настройки для локального интерфейса и убедитесь, что они соответствуют зарезервированным.
Остановите сервис dhcpd на узле host1. На узле host3 удалите информацию о всех полученных арендах. Переполучите настройки сетевых интерфейсов. Убедитесь, что настройка локального интерфейса закончится ошибкой.
На узле host2.
 1. Сконфигурируйте локальный интерфейс с использованием файлов описания сетевых настроек. Добавьте в файл /etc/sysconfig/network следующую строку: GATEWAY=10.0.0.(N+1). Убедитесь, что после перезапуска /etc/init.d/network интерфейс будет сконфигурирован корректно.
 2. Установите и настройте dhcp сервер так, чтобы он отвечал на запросы из сетей 10.0.0.0/28 и 172.16.[(N+1)*10].0/24. Сервер должен "прослушивать" только внешний интерфейс (задаётся в файле /etc/sysconfig/dhcp). Параметры областей следующие:
 1. Область 10.0.0.0/28 - пустая (нет ни каких настроек)
 2. Область 172.16.[(N+1)*10].0:
 - адреса выдаются из диапазона от 230 до 240.
 - шлюз по умолчанию - 172.16.[(N+1)*10].2.
 3. Настройте агента ретрансляции таким образом, чтобы он передавал все запросы на автоматическую конфигурацию сетевых интерфейсов узлу с адресом 10.0.0.[(N-1)*10].
 4. Запустите сервис dhcprelay. Настройте его таким образом, чтобы он запускался автоматически при загрузке системы на уровень 3.

На узле host3 переполучите настройки сетевых интерфейсов. Убедитесь, что настройка локального интерфейса получена от DHCP сервера из соседней сети.

Контрольные вопросы

1. Что такое DHCP? Необходим ли подобный сервис в локальных сетях?
2. Опишите назначение пакетов: DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK, DHCPNACK, DHCPINFORM.
3. Зачем нужен dhclient?
4. Что такое класс клиента? Как можно задать класс клиента при использовании пакета dhclient?
5. Что такое диапазон адресов (range)?
6. Как используется резервирование и зачем?
7. Как указать в настройках сетевой конфигурации узла host3 какой из интерфейсов использовать для передачи данных "по умолчанию"?
8. Зачем используется агент ретрансляции?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А. Мельникова

Практическое занятие 31

Управление учетными записями пользователей

Цель работы: Изучить какими правами обладают различные группы пользователей и обучить научить работать с правами групп пользователей.

Оснащение: МУ к ПЗ

Описание работы:

Обычно разрешение на выполнение тех или иных действий выдается по результатам сравнения списка контроля доступа, связанного с объектом, с идентификаторами безопасности пользователя и групп, членом которых является пользователь.

Однако некоторые действия пользователя не связаны с объектами Windows 7. Например, чтобы определенные сотрудники могли делать резервные копии дисков сервера они должны иметь право копировать файлы независимо от того, есть ли у них разрешение *на* это в списке контроля доступа. В этом случае пользователям предоставляются специальные *права* (UserRights).

В диалоговом окне Локальные Параметры Безопасности, вызываемом через *Панель Управления*, для каждого из специальных прав определенных в системе, администратор составляет список пользователей и групп, которым предоставлено это право.

Основные права пользователя

Manage auditing and log (SeSecurityPrivilege security)	... указать, какие типы ресурсов должны подвергаться аудиту, а также просматривать и очищать журнал безопасности. Это право, однако, не позволяет устанавливать системные правила. Пользователей, обладающих данным правом, можно обозначить как аудиторов.
Restore files and directories (SeRestorePrivilege)	... используя резервную копию, восстановить файлы и папки в обход разрешений файловой системы. Эта привилегия, кроме того, включает в себя право устанавливать любое значение в поле <i>владелец</i> (Owner) ресурса.
Shut down the system (SeShutdownPrivilege)	... остановить работу Windows NT.
Take ownership of files or other objects (SeTakeOwnershipPrivilege)	... стать владельцем объекта независимо от разрешений, связанных с объектом. Это право позволяет в конечном итоге поменять любые разрешения, приписанные объекту.

Право	Дает пользователю возможность...
Log on locally	... войти в систему локального компьютера с использованием клавиатуры.
Access this computer from the network	... подключиться к компьютеру по сети.
Back up files and directories (SeBackupPrivilege)	... делать резервные копии файлов и каталогов в обход разрешений файловой системы.
Change the system time (SeSystemTimePrivilege)	... менять системное время компьютера.
Force shutdown from a remote system (SeRemoteShutdownName)-	... завершить работу системы с удаленного компьютера.
Load and unload device drivers (SeLoadDriverPrivilege)	... загружать и выгружать драйверы устройств.

Списки пользователей и групп, можно увидеть Пуск/Настройки/Панель Управления/ Учетные Записи Пользователей, либо , набрав в окне Выполнить: controluserpasswords2. Список прав пользователей находится Пуск/ Настройки/ Панель Управления/ Администрирование/ Локальная Политика Безопасности (папка *Администрирование* видна только если *Панель Управления* приведена к классическому виду). Это меню позволяет давать права и привилегии пользователям. Окно свойства позволяет видеть список правообладателей и вносить в него новых пользователей. Windows 7 позволяет экспортировать список (создавать резервную копию списка).

Четыре из перечисленных выше прав - Logonlocally, Accessthiscomputerfromthenetwork, Logonasaservice и Logonasabatchjob - действуют особо. Они позволяют создавать для пользователя

маркеры доступа определенного типа и тем самым определяют, какого типа вход в систему разрешен пользователю.

Остальные права являются в действительности системными привилегиями (privileges). Привилегии пользователя заносятся в маркер доступа. В дальнейшем, прежде чем выполнить некоторый привилегированный запрос, операционная система проверит, что маркер доступа, связанный с издавшим запрос процессом, содержит соответствующую привилегию.

Создание новых групп пользователей осуществляется через Пуск/Настройки/Панель Управления/Администрирование/Управление Компьютером/ Локальные Пользователи и Группы: меню Действие, вкладка Создать группу. Windows 7 содержит и более простое средство создания новых учетных записей пользователей – папка *Учетные Записи Пользователей*. С её помощью можно создавать и изменять учетные записи пользователей и изменять вход пользователей в систему.

Порядок выполнения работы:

1. Изучить теоретическую часть.
1. Выполнить задания.
1. Предоставить отчет о проделанной работе.
2. Ответить на контрольные вопросы.

Контрольные вопросы:

1. Какая программа используется для модификации прав доступа группы?
1. Может ли пользователь группы Users завершить работу с удаленного компьютера?
1. Какая группа (группы) может стать, владельцем объекта независимо от разрешений, связанных объектом?
 1. Может ли от имени пользователя зарегистрироваться служба.
 2. Если администратор воспользовался правом Takeownership, может ли владелец ресурса обнаружить попытку доступа к своей информации?
 3. Каким способом можно отследить использование привилегии Takeownership? И что для этого нужно сделать.

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учрежд. СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 32

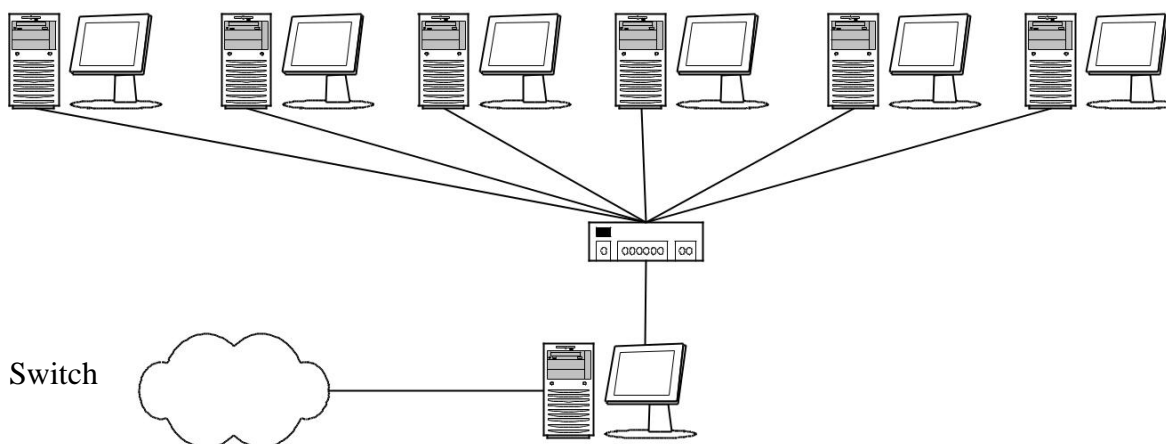
Настройка доступа к сети Интернет из локальной сети

Цель работы: Рассмотреть различные варианты подключения к сети Интернет локальной сети, используя различные программные средства.

Оснащение: Имеется локальная сеть (*Workstation 1 – Workstation 2*) представленная на рисунке. На компьютере(шлюзе), через который планируется подключение локальной сети к Интернет необходимо наличие двух сетевых адаптеров (подключений).

Задание: Необходимо обеспечить доступ к сети Интернет со всех рабочих станций.

Workstation 2 Workstation 3 Workstation 4 Workstation 5 Workstation 6 Workstation 7



Internet

Workstation 1

Краткие теоретические сведения:

Имеются три основных варианта подключения локальной сети к Интернет:

1. «прямое» IP-подключение,
2. подключение через NAT,
3. подключение через прокси-сервер.

Рассмотрим преимущества, недостатки и область применения каждого метода, а также некоторые возникающие нюансы. Выбор конкретного способа подключения зависит от потребностей пользователей, цели подключения и, в некоторой степени, финансовых возможностей.

Итак, компьютер *Workstation 1*. У него есть доступ, как к Интернету, так и к локальной сети. Наша задача - дать компьютерам локальной сети доступ к Интернет через подключенный к нему компьютер. Далее этот компьютер мы будем называть шлюзом или маршрутизатором.

Рассмотрение способов мы начнем с наименее часто используемого, наиболее дорогого, но также наиболее «правильного» и естественного способа, дающего наибольшие по сравнению с другими способами возможности. **«Прямое» IP-подключение к Интернет.** Для того, чтобы Ваша локальная сеть была полноценно подключена к Интернету, должны соблюдаться, как минимум, три условия:

1. Каждая машина в локальной сети должна иметь "реальный", интернетовский IP-адрес;
2. Эти адреса должны быть не любыми, а выделенными Вашим провайдером для Вашей локальной сети (скорее всего, это будет подсеть класса C);
3. На компьютере-шлюзе, подключенном к двум сетям - локальной сети и сети провайдера, должна быть организована IP-маршрутизация, т.е. передача пакетов из одной сети в другую.

В этом случае Ваша локальная сеть становится как бы частью Интернета. Собственно, это тот способ подключения, которым подключены к Интернету сами Интернет-провайдеры и хостинг-провайдеры.

В отличие от обычного подключения, рассчитанного на один компьютер, при таком подключении "под клиента" выделяется не один IP-адрес, а несколько, так называемая "IP-подсеть".

При таком способе подключения Вы можете организовать в своей сети сервисы, доступные из Интернета - ведь при данном подключении не только Интернет полностью доступен из Вашей сети, но и Ваша сеть - из Интернета, т.к. является его частью.

Однако такая "прозрачность" Вашей сети резко снижает ее защищенность - ведь любые сервисы в локальной сети, даже предназначенные для "внутреннего" использования, станут доступными извне через Интернет. Чтобы это не имело места, доступ в локальную сеть извне несколько ограничивают. Обычно это делается установкой на шлюзе программы-firewall. Это своеобразный фильтр пакетов, проходящих из одной сети в другую. Путем его настройки можно запретить вход-выход из локальной сети пакетов, соответствующих определенным критериям - типу IP-пакета, IP-адресу назначения, TCP/UDP-порту и т.п.

Firewall решает такие задачи, как:

1. блокировку доступа извне к определенным TCP/IP-сервисам локальной сети.
2. блокировку доступа к определенным компьютерам локальной сети. Таким образом, можно запретить доступ извне ко всем машинам, кроме определенных серверов, предназначенных для доступа из Интернет.
3. защиту от троянских программ на сетевом уровне.

Несмотря на универсальность такого метода подключения локальной сети к Интернет, этот метод имеет недостатки. Благодаря им, его реально и используют только лишь те организации, которым надо сделать свои сервера доступными из Интернет - в основном, те же интернет-провайдеры и хостинг-провайдеры, а также информационные службы. Самый главный недостаток заключается в дороговизне выделения IP-адресов и уж тем более IP-подсетей, к тому же эту плату надо вносить периодически.

Поэтому на практике рассмотрим другие, описанные далее способы, не требующие больших затрат и, что самое главное, позволяющие подключить локальную сеть через обычное подключение с одним внешним IP-адресом.

Настройка подключения через Win7. Прокси-сервер

На первом этапе необходимо установить прокси сервер на компьютере подключенном к сети Интернет. Используйте дискету или флешку для переноса программы.

Установите и настройте программу.

Настройка подключения через Win7. NAT

Попробуйте самостоятельно настроить этот режим **Вывод**. Теперь Вы должны суметь построить сеть из нескольких компьютеров, а также организовать доступ к сетиInternet.

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 33

Установка и обновление программных пакетов

Цель работы: Получить базовые знания управления процессом установки, программных пакетов.

Оснащение: МУ к ПЗ

Краткие теоретические сведения:

Необходимость в установке новых программных пакетов под LINUX возникает в двух основных случаях:

когда появляется новая версия одного из уже установленных у вас пакетов;

когда возникает желание или необходимость использовать какой-то пакет, еще не установленный в системе.

Во втором случае это может быть один из пакетов, имеющихся на вашем установочном диске, но не установленный в процессе инсталляции. Однако чаще всего новое ПО вы будете находить в Интернете, тем более, что значительная часть этого ПО бесплатна. Как бы то ни было, но рано или поздно вы все равно окажетесь перед необходимостью установить новый пакет.

Для дистрибутивов, основанных на Red Hat Linux, существует две основных формы распространения ПО: в исходных текстах и в виде исполняемых модулей. В первом случае пакет ПО обычно поставляется в виде tar-gz архива, во втором случае - в виде rpm-пакета (но это не обязательно, исполняемые модули также могут распространяться в виде tar-gz-архива).

Проще всего установить ПО, представленное в виде rpm-пакета, содержащего исполняемые файлы, этот способ мы и рассмотрим. Отметим только, что для инсталляции новых пакетов вы должны войти в систему как пользователь root.

Программа rpm

Название этой программы (или команды) является аббревиатурой от Redhat Package Manager. Преимуществом использования этой программы по сравнению с установкой tar gz архивов является то, что она автоматически проделает все необходимые действия по установке ПО: создаст необходимые каталоги, распределит по ним файлы, создаст ссылки. Кроме того, она может быть использована не только для установки нового пакета, но и для обновления версий ПО, получения перечней установленного ПО и проверки установки, а также для деинсталляции отдельных пакетов (например, если после периода пробной работы с программой вы решили отказаться от ее дальнейшего использования).

Если вы желаете установить совершенно новый пакет (у вас не было на компьютере предыдущих версий этого ПО), то для установки пакета из этого архива достаточно перейти в тот каталог, где находится архив, и дать команду:

```
rpm -i имя_rpm-архива
```

Если у вас была установлена предыдущая версия пакета, то в простейшем случае надо дать команду следующего формата:

```
rpm -U --force имя_rpm-архива
```

Здесь параметр -U говорит программе, что надо произвести обновление (upgrade) пакета, а опция --force требует безусловно (и без лишних вопросов) обновить все входящие в пакет файлы. Заметьте, что это очень сильное требование, и в некоторых случаях может быть лучше сохранить какие-то (например, конфигурационные) файлы от предыдущей версии.

Программа rpm позволяет выяснить, какие файлы установит тот или иной пакет. Для этого надо дать следующую команду (только учтите, что текущим должен быть каталог, содержащий интересующий вас пакет):

```
rpm -qpl имя_rpm-архива
```

А для получения информации о том, для чего служит ПО, содержащееся в rpm-пакете, используйте команду

```
rpm -qri имя_rpm-архива
```

Дело в том, что файлы RPM кроме собственно архива файлов содержат информацию о пакете, включая имя, версию и краткое описание. С помощью той же программы rpm вы можете просмотреть эту дополнительную информацию.

Если дать команду: `rpm -qrl имя_rpm-архива` будет выдан список входящих в пакет файлов с указанием того, куда они будут установлены.

По команде `rpm -qa` вы получите перечень всех установленных в системе пакетов.

Вы можете искать информацию об отдельном пакете или об отдельных файлах. Например, вы можете легко найти, какому пакету принадлежит файл и откуда появился.

Команда `rpm -qf путь_к_файлу`

Если вы беспокоитесь о том, что случайно удалили важный файл из установленного пакета, просто проверьте это:

`rpm -Va`

Вы будете оповещены об любых аномалиях. Потом можно переустановить пакет, если это необходимо. Любые конфигурационные файлы будут сохранены.

Как видите, `rpm` это очень полезная утилита, и у нее имеется много разных опций.

Всего `rpm` имеет 16 основных режимов работы, которые можно объединить в 6 групп:

Запросы

Запрос: `rpm [--query] [queryoptions]`

Показать метки запросов (Querytags): `rpm [--querytags]`

Установка и поддержка установленных пакетов

Установка: `rpm [--install] [installoptions] [package_file]+`

Обновление: `rpm [--freshen|-F] [installoptions] [package_file]+`

Деинсталляция: `rpm [--uninstall|-e] [uninstalloptions] [package]+`

Проверка: `rpm [--verify|-V] [verifyoptions] [package]+`

Подписи (пакеты подписываются электронной цифровой подписью в формате PGP, с целью обеспечения неизменяемости и сохранения авторства пакетов).

Проверка подписи: `rpm [--verify|-V] [verifyoptions] [package]+`

Переподписывание: `rpm [--resign] [package_file]+`

Добавление подписи: `rpm [--addsign] [package_file]+`

Работа с базой

Инициализация базы: `rpm -i [--initdb]`

Обновление базы (Rebuild Database): `rpm -i [--rebuilddb]`

Создание rpm-пакетов

Создать пакет: `rpm [-b|t] [package_spec]+`

Перекомпилировать пакет: `rpm [--rebuild] [sourcerpm]+`

Скомпилировать пакет из tar-архива: `rpm [--tarbuild] [tarredsource]+`

Разное

Показать конфигурацию программы `rpm`: `rpm [--showrc]`

Задать пользователей: `rpm [--setperms] [package]+`

Задать группы: `rpm [--setgids] [package]+`

Ход работы: Для настройки файлового сервера нам необходимо установить соответствующие пакеты

Примонтируйте CD-ROM (вспомните задания лабораторной «Управление файловой системой»).

На одном из установочных дисков в каталоге

`rpm -ihv samba...`

`rpm -ihv system-config-samba...`

Настроить конфигурационный файл `/etc/samba/smb.conf`.

Пример конфигурационного файла для настройки файлового сервера:

=====
=====
[global]

Контрольные вопросы:

1. Какое назначение пакета samba?
1. Какой общий порядок настройки файлового сервера?
2. Какие основные возможности программы grm?
3. Какая команда добавляет нового samba-пользователя?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 34

Настройка файлового и веб-сервера

Цель работы: получить теоретические и практические навыки по работе с веб-сервером

Оснащение: МУ к ПЗ, ПК

Порядок выполнения работы

Краткие теоретические сведения

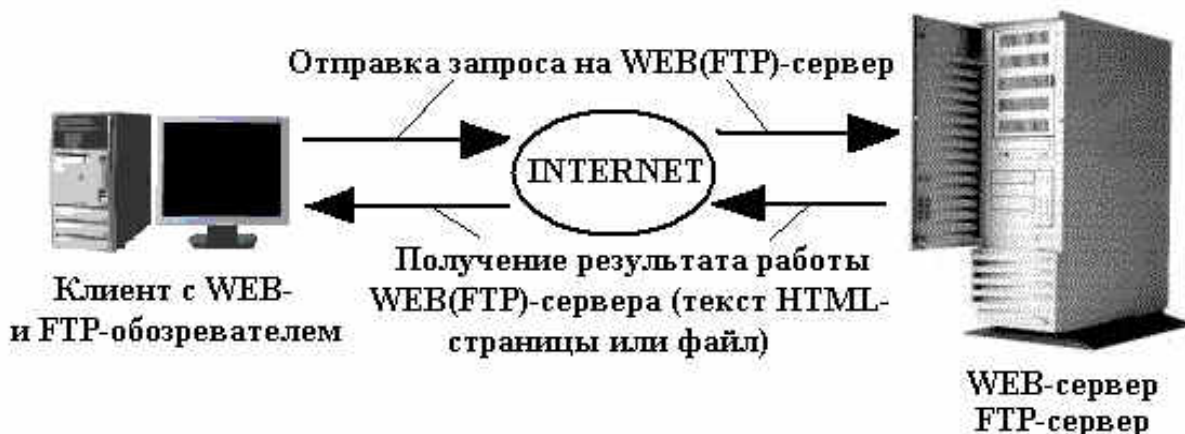
Веб-сервер — это сервер, принимающий HTTP-запросы от клиентов, обычно веб-браузеров, и выдающий им HTTP-ответы в виде HTML-страницы с изображениями, текстами, медиа-поток или другими данными. Веб-серверы это основа Всемирной паутины WWW.

Веб-сервером называют как программное обеспечение, выполняющее функции **веб-сервера**, так и компьютер, на котором это программное обеспечение работает.

Клиенты получают доступ к **веб-серверу** по URL адресу нужной им **веб-страницы** или FTP ресурса.

FTP ресурс использует **FTP (англ. File Transfer Protocol — протокол передачи файлов)** протокол, предназначенный для передачи файлов в компьютерных сетях. **FTP** позволяет подключаться к серверам **FTP**, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

Схема работы WEB- и FTP-сервера.



Установка WEB - и FTP-сервера.

1. Скачайте на диск компьютера программное обеспечение WEB- и FTP- сервера, находящееся по адресу <ftp://10.242.48.45/software/Xitami/xitami.zip> Этот файл представляет собой дистрибутив программного обеспечения WEB- и FTP- сервера, упакованный в виде архива ZIP.

1. Дважды щелкнув в «Проводнике» по файлу **xitami.zip** откройте архив. Скопируйте содержимое каталога **xitami** из архива на диск **D:\famili** компьютера. Вместо **famili** создайте папку со своей фамилией (латинскими буквами и без пробелов).

Установка WEB- и FTP – сервера завершена. Теперь его необходимо настроить для работы.

Проверка работы WEB-сервера.

1. Откройте новое окно обозревателя Internet Explorer

1. Введите в адресной строке адрес WEB-сервера вашего партнера, на который вы загрузили HTML-страницу. Адресная строка имеет вид: `http://IP-адрес/`

2. Если вы все сделали правильно, должна открыться страница, которую вы загрузили на WEB-сервер вашего партнера. **На закрывайте это окно.**

Если страница не открылась.

1. Проверьте, правильно - ли введен адрес сервера.

1. Подключитесь к серверу через FTP и заново загрузите HTML-страницу на сервер.

2. Если по - прежнему страница не открывается, возможно у партнера неправильно настроен WEB(FTP)-сервер. Сообщите ему об этом.

Проверка работы анонимногоFTP-сервера.

1. Откройте новое окно обозревателя Internet Explorer

1. Введите в адресной строке адрес FTP-сервера вашего партнера, на который вы загрузили файлы в его файловый архив. Адресная строка имеет вид: ftp://IP-адрес/
2. Должен открыться список файлов, находящихся в файловом архиве. Загрузите какой-нибудь файл дважды щелкнув по нему мышкой.
3. Попробуйте удалить один из файлов с сервера. В режиме анонимного доступа файлы не должны удаляться и быть доступными только для чтения. Если файлы удаляются, сообщите партнеру о неправильной настройке анонимного доступа.

Если файловый архив не открывается.

1. Проверьте, правильно - ли введен адрес сервера.
1. Если по - прежнему файловый архив не открывается, возможно у партнера неправильно настроен FTP-сервер. Сообщите ему об этом.

Работа с WEB-сервером через его доменное имя.

1. Откройте обозреватель Internet Explorer
1. Введите в адресную строку доменное имя вашего сайта. Доменное имя имеет вид <http://wXX.stucity.ru>, где XX – последняя цифра IP-адреса вашего сервера. Например, если ваш IP-адрес 10.242.48.40, тогда доменное имя будет w40.stucity.ru

Пригласите преподавателя и покажите ему два окна обозревателя InternetExplorer:

1. С открытой HTML-страницей
1. С открытым файловым архивом.
2. Объясните преподавателю, как работает система доменных имен (почему вы работаете с доменным именем и открывается ваш сайт).

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 35

Автоматизация процесса администрирования

Цель работы: установка, конфигурирование и администрирование средств удаленного доступа в корпоративной сети. Необходимо установить VNC сервер в операционной системе Linux, установить клиенты для подключения к VNC серверу в ОС Windows Server 2008 R2, Windows 7.

Настроить Windows Server 2008 для подключения по протоколу RDP – пользователями ОС Astra Linux и Windows 7. Настроить Windows 7 для удаленного подключения пользователями ОС Astra Linux Common Edition и Windows Server.

Последовательность выполнения лабораторной работы

Создать три виртуальные машины с именами Linux, Server и Win7. Все компьютеры имеют доступ к частной сети. Операционные системы: Linux - ОС Astra Linux Common Edition, Server - ОС Windows Server 2008 R2 и Win7 - Windows 7. Операционные системы загружаются с разностных дисков (требуется создать самостоятельно), в качестве родительских дисков выступают VHD диски с установленными операционными системами, которые использовались при выполнении предыдущих лабораторных работ.

Установить IP адреса и имена компьютеров в ОС следующие ОС Astra Linux Common Edition – имя, как и в первой лабораторной работе, IP 192.168.1.3, Windows Server 2008 R2 – имя Server, 192.168.1.1, Windows 7 – имя Win7, 192.168.1.2. Маска сети 255.255.255.0.

ОС Windows Server 2008 R2 и Windows 7 – члены рабочей группы IS

Выполнить настройку доступа по RDP на Windows Server 2008 R2 и Windows 7.

Создать виртуальный жесткий диск lab3.vhd. Записать на него файлы.

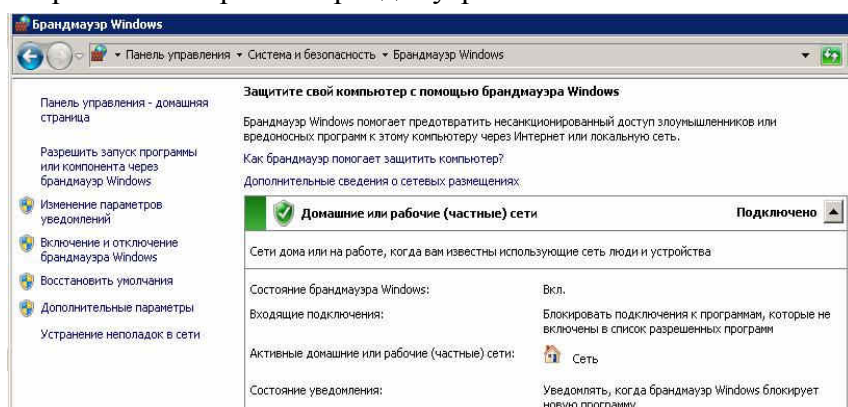
Имя	Дата изменения	Тип	Размер
Remmina-1.0.0.tar.gz	15.10.2014 1:16	Архив WinRAR	528 КБ
Remmina-1.0.0.zip	15.10.2014 1:16	Архив ZIP - WinRAR	768 КБ
UltraVNC_1_2_03_X64_Setup.exe	14.10.2014 22:51	Приложение	2 901 КБ
UltraVNC_1_2_03_X86_Setup.exe	14.10.2014 22:50	Приложение	3 299 КБ

Сделать 2 копии данного файла, переименовать lab3-linux.vhd и lab3-windows.vhd. Смонтировать диски lab3-linux.vhd в ОС Astra Linux Common Edition и lab3-windows.vhd в Windows Server 2008 R2 (диск D).

В Установить Ultra VNC (клиент и сервер) в ОС Windows Server 2008 R2

0. Windows 7. Выполнить настройку, проверить работоспособность (с ОС Windows Server 2008 R2 подключится к Windows 7 и наоборот).

Обратить внимание на правила настройки брандмауэра Windows.



Выполнить установку VNC сервера в ОС Astra Linux. Использовать команду `apt-get install vnc4server` (если работаете, как суперпользователь `root` или `sudo apt-get install vnc4server`). Рассмотреть и описать параметры настройки.

Выполнить настройку сервера, варианты подключения с компьютеров ОС Windows Server 2008 R2 и Windows 7 – с использованием клиента

Ultra VNC и по http протоколу. Сделать скриншоты, описать настройки, возможные проблемы подключения и способы их решения.

Выполнить настройку клиента на компьютере ОС Astra Linux для подключения к ОС Windows Server 2008 R2 и Windows 7. Для этого использовать инструмент Remmina:

Remmina поддерживает большое количество протоколов удаленного подключения RDP, RDPF, RDPS, SFTP, SSH, VNC и VNCI. Список поддерживаемых протоколов можно расширить с помощью плагинов.

Все добавленные компьютеры для удаленного соединения можно объединить в группы.

Простой и удобный вкладочный интерфейс.

В полноэкранный режим для удобства добавляется плавающая панель, на которой расположены наиболее востребованные инструменты.

В Remmina можно редактировать список доступных разрешений удаленных машин. Позволяет включить практически любое разрешение, что сказывается на удобстве работы с помощью нетбука.

Есть настраиваемые горячие клавиши.

В Remmina есть возможность "жестко" указать раскладку языка клавиатуры.

Есть возможность гибко настроить скорость/качество соединения, регулируя на удаленной машине отображение анимации меню, отображение тем оформления, фона рабочего стола, применяемого

Compiz и т.д.

В Remmina можно указать общие ресурсы (директорию или принтер), которые будут видны на удаленном компьютере.

В Remmina можно включить/отключить синхронизацию буфера обмена.

Запустить выбранную программу при загрузке сессии в терминальном режиме.

Выполнить команду `apt-get install remmina`. Удалось ли установить пакет? Рассмотреть файлы remmina на смонтированном диске lab3-linux.vhd, попробовать выполнить процесс установки. Удалось? Проблемы? Описать процесс конфигурирования. В случае необходимости скачать необходимый для установки дистрибутив remmina с сайта разработчика. Для информации

Установка itshaman.ru/it-programmy-dlya-linux/214/remmina-udobnyj-rdp-klient-dlya-linux

1. Загрузить исходный код RPM- или DEB-пакеты вручную можно с [официальной странички на sourceforge.net](http://sourceforge.net).
2. Установить Remmina в Ubuntu последней версии можно из дополнительного репозитория на launchpad.net.

```
# sudo add-apt-repository ppa:llyzs/ppa & # Подключение дополнительного
sudo apt-get update                    репозитория launchpad.net

# sudo apt-get install remmina remmina- # Устанавливаем Remmina
gnome
```

Если для подключения к Интернет Вы используете прокси-сервер, то подключить дополнительный репозиторий в Ubuntu Вы можете вторым способом.
Спойлер: Второй способ установки Remmina.

```
# echo "deb
http://ppa.launchpad.net/llyzs/ppa/ubuntu # Подключение дополнительного
`lsb_release -cs` main" | sudo tee -a репозитория launchpad.net
/etc/apt/sources.list

# sudo apt-key adv --keyserver
keyserver.ubuntu.com --recv-keys # Установка ключа авторизации и
D7260B8F5AoFASF1 && sudo apt-get обновление списка пакетов
update

# sudo apt-get install remmina remmina- # Устанавливаем Remmina
```

10. Установить сервер OpenSSH на компьютер ОС Astra Linux. Используя клиент, подключиться к серверу OpenSSH с компьютера Win7. На компьютере Win7 на диске C создать папку 1. В эту папку скопировать, используя возможности OpenSSH с компьютера с ОС Astra Linux



Выводы по работе – сравнить использованные технологии, привести примеры программных средств, аналогичных использованным. Достоинства, недостатки, особенности конфигурирования и лицензирования.

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 36

Автоматизация процесса резервирования данных

Цель работы: Получить навыки архивирования и восстановления системы, используя стандартные утилиты Windows Server 2003. Решить задачи сетевого администратора связанные с сохранением, архивированием информации, и ее последующим восстановлением.

Дано: Имеется локальная сеть с контроллером домена на базе ОС Windows 2003 Server.

Задание: Необходимо, используя стандартные утилиты Windows Server 2003 обеспечить архивирование и восстановления системы, а также настроить механизмы резервирования важных данных.

Краткие теоретические сведения:

Ни один носитель информации не является абсолютно надежным, из строя может выйти любое устройство хранения данных, и данные могут быть потеряны. Кроме аппаратных сбоев возможна также потеря данных по причине действия вредоносных программ (вирусы и т.п.). А самая распространенная причина порчи или удаления данных — ошибки пользователей (как обычных, так и администраторов), которые могут по ошибке удалить или перезаписать не тот файл.

По этой причине возникает необходимость регулярного создания резервных копий информации — файлов с документами, баз данных и состояния операционной системы.

Системы семейства Windows Server имеют встроенный инструмент создания резервных копий — утилиту *ntbackup*. Данная утилита позволяет сохранять резервные копии на самых различных носителях — ленточных накопителях, магнитооптических дисках, жестких дисках (как на локальных дисках данного сервера, так и на сетевых ресурсах, размещенных на других компьютерах сети). В версии системы Windows 2003 реализован механизм т.н. теневых копий *Shadow Copy*, который заключается в том, что в начале процедуры архивации система делает моментальный «снимок» архивируемых файлов и уже после этого создает резервную копию из этого снимка. Данная технология позволяет архивировать файлы, которые в момент запуска утилиты *ntbackup* были открыты пользователями.

Сетевой администратор должен совместно с пользователями определить те данные, которые нужно регулярно архивировать, спланировать ресурсы, необходимые для создания резервных копий, составить расписание резервного копирования, настроить программу резервного копирования и планировщик заданий для автоматического создания резервных копий. Кроме этого, в задачу сетевого администратора входит также регулярное тестирование резервных копий и пробное восстановление данных из резервных копий (чтобы вовремя обнаружить возникающие проблемы в создании резервных копий).

Архивирование и восстановление файловых ресурсов. Базовые понятия службы резервного копирования

Все операции по созданию резервных копий и восстановлению данных в ОС семейства Windows осуществляются утилитой *ntbackup*.

Рассмотрим основы резервного копирования файловых ресурсов. Каждый файл, хранящийся на диске компьютера, независимо от типа файловой системы, имеет атрибут *archive*, который в Свойствах файла отображается как «Файл готов для архивирования» (откройте Свойства файла и нажмите кнопку «Другие»). Если в Свойствах файла вручную убрать галочку у этого атрибута, то при любом изменении в файле операционная система автоматически снова установит этот атрибут. На использовании изменений данного атрибута основаны все используемые в системе Windows методики резервного копирования.

Типы резервного копирования

Утилитой *ntbackup* можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

Обычный (Normal)

При выполнении данного типа архивирования утилита *ntbackup* архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут «Файл готов для архивирования». Данный вид архивирования необходим для создания еженедельных

полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

Разностный (Differential)

При выполнении Разностного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут не очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) — Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования «Обычный + Разностный» процесс восстановления данных в случае утери информации потребует выполнения двух операций восстановления — сначала из последней Полной копии, а затем из последней Разностной резервной копии.

Добавочный (Incremental)

При выполнении Добавочного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут «Файл готов для архивирования», при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации «Обычный + Добавочный» уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

Копирующий (Copy)

При таком типе архивирования утилита *ntbackup* заархивирует все отмеченные файлы, при этом атрибут «Файл готов для архивирования» остается без изменений.

Ежедневный (Daily)

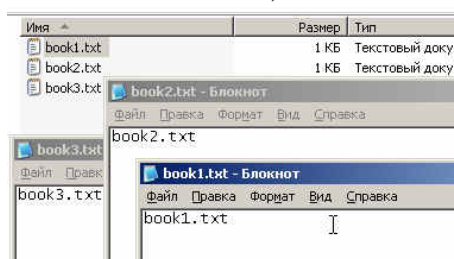
Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Ход работы:

Создания задания на выполнения архивации данных

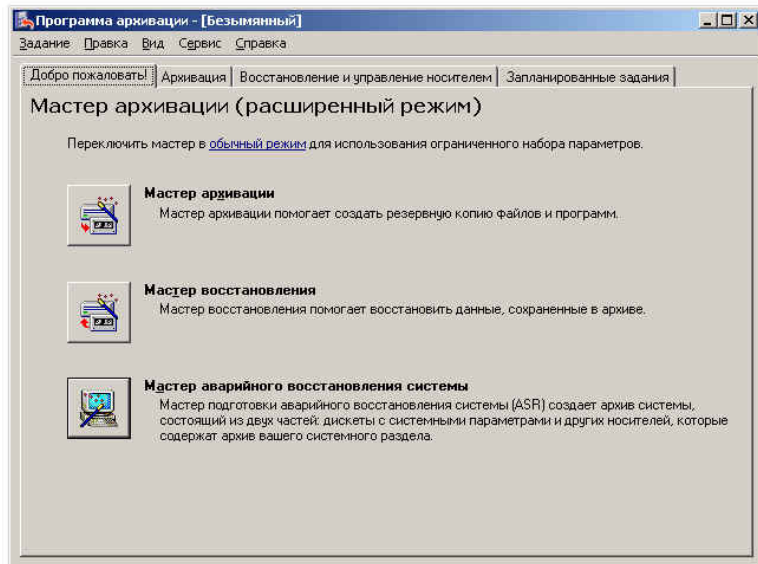
1. Создать на диске «С» Вашего сервера каталог *backup* и *restore*;
1. В папке *library*, созданной в одной из предыдущих работ создать 3 текстовых файла с наименованиями *book1.txt*, *book2.txt* и *book3.txt*. Файлы должны содержать свое наименование.



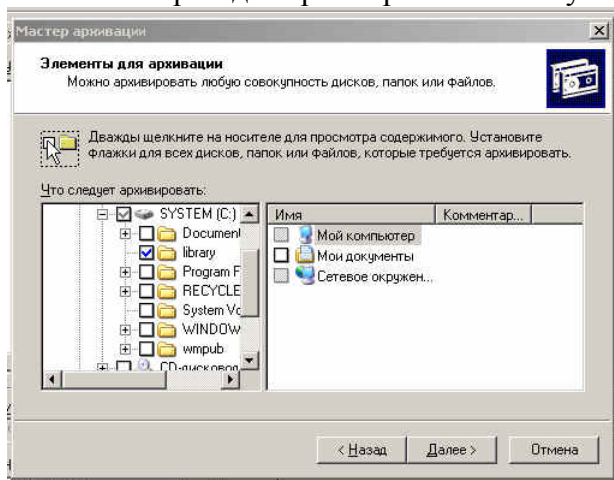
2. Запустить утилиту резервного копирования *ntbackup*.

Эту утилиту можно запустить из Главного меню системы (кнопка «Пуск» — «Все программы» — «Стандартные» — «Служебные» — «Архивация данных»), а можно запустить более быстро из командной строки (кнопка «Пуск» — «Выполнить» — «*ntbackup*» — кнопка «ОК»). При первом запуске утилиты рекомендуем убрать галочку у поля «Всегда запускать в режиме мастера».

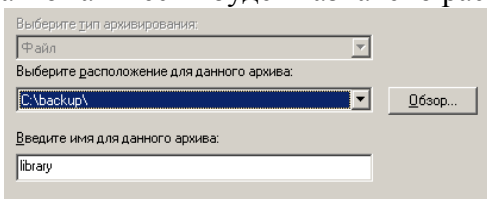
3. Запустить «Мастер архивации» (на закладке «Добро пожаловать» нажать кнопку «Мастер архивации».



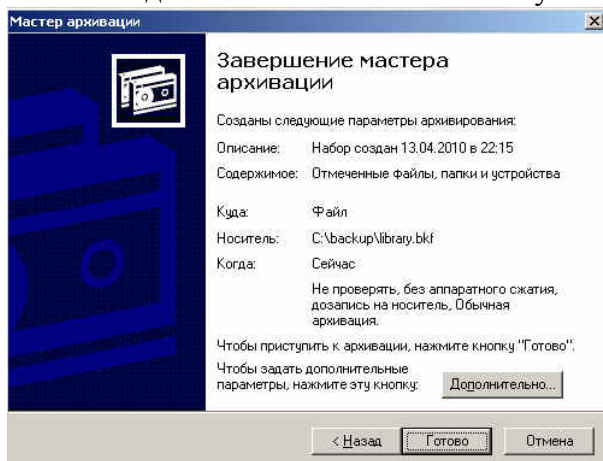
4. После запуска мастера нажмем кнопку «Далее» и выберем, что нам нужно архивировать, в данном примере — «Архивировать выбранные файлы, диски или сетевые данные»
5. Выберем для архивирования папку *library*.



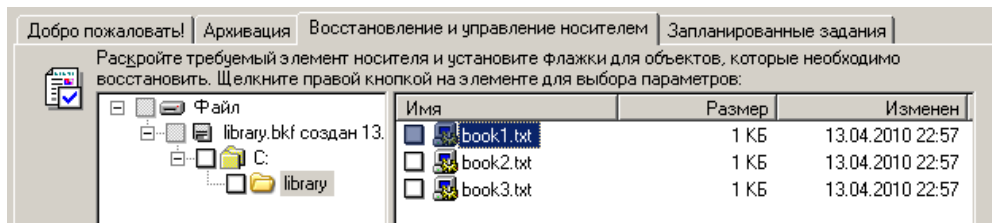
6. Выберем место для создания резервной копии, создадим файл с именем *library*, этому файлу автоматически будет назначено расширение «*.bkf*»



7. На данном этапе нажмем кнопку «Готово».

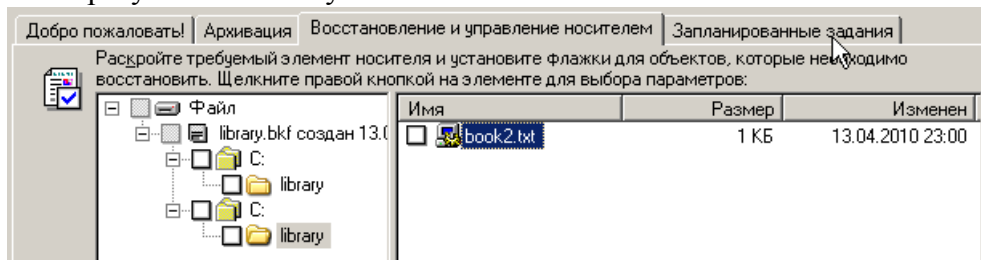


8. Проверяем полученный результат.



9. Вносим изменение в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут «Файл готов для архивирования», а *book3.txt* - удаляем.

10. Запускаем снова процесс архивации, но на 8 этапе нажмем кнопку «Дополнительно», чтобы задать дополнительные параметры и выбираем тип архивации «Добавочный». Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. Почему он такой?

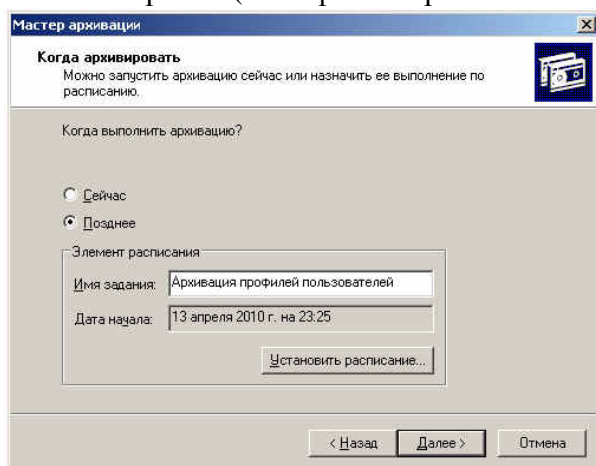


11. Восстановите файл *book3.txt*. Для этого выполните следующие действия:

- Запустим утилиту резервного копирования *ntbackup*.
- Перейдем на закладку "Восстановление и управление носителем".
- После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("Исходное размещение") или выбрать иной путь для их сохранения ("Альтернативное размещение"). Выберите папку *restore*.
 - После определения всех параметров восстановления нажмем кнопку "Восстановить", утраченные данные будут восстановлены.

12. Создайте задания на выполнения архивации данных для папки *profiles*, используя выбор дополнительных возможностей:

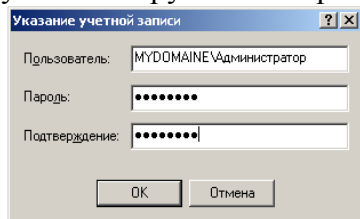
- Выбираем тип архивирования (выберем «Обычный»).
- Ничего не меняем на странице «Способы архивации».
- На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).



13. На странице «Когда архивировать» задайте расписание для автоматического создания резервной копии — выберите вариант «Позднее» и задайте расписание архивирования, чтобы архивирование происходило по всем рабочим дням недели. Время начала установите, исходя из текущего времени системы + пять минут.

14. Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями

будет выполняться задание архивирования. Рекомендуем для выполнения заданий резервного копирования создать специальные учетные записи, обладающие достаточными правами (как минимум члены группы «Операторы архива»).



15. Нажмем кнопку «Готово», задание будет создано, и оно появится в списке «Назначенных заданий». Теперь оно будет выполняться регулярно в соответствии с расписанием.

16. Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

Теневые копии

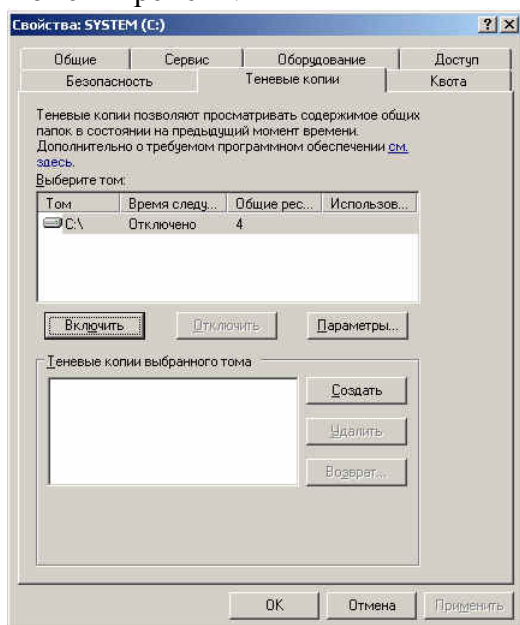
Эта технология, реализованная в Windows 2003, позволяет архивировать открытые файлы с помощью создания «снимка» файловых ресурсов. По умолчанию теневые копии создаются на том же томе, где хранятся сетевые папки, поэтому они не смогут стать серьезной защитой от аппаратных аварий (например, выход из строя диска, на котором размещены эти данные). Можно настроить создание теневых копий на другом томе, что повысит уровень защиты. Теневые копии позволяют восстанавливать данные, ошибочно удаленные или модифицированные пользователями. При этом пользователи могут восстанавливать данные сами, без участия системного администратора. Теневые копии создаются только на томах с файловой системой NTFS.

Рассмотрим пример создания и использования теневых копий тома.

1. Создадим в сетевой папке на сервере файл *document.txt*, содержащий текст: «11111».

1. Откроем Свойства какого-либо тома и перейдем на закладку «Теневые копии». По умолчанию создание теневых копий для всех томов отключено.

2. Включим создание теневых копий для тома «С». При этом автоматически создастся первая теневая копия. В этом окне также можно вручную создать теневую копию данного тома в любой момент времени.



3. Настроим параметры теневого копирования. Для хранения теневых копий на томе требуется не менее 100 МБ дискового пространства, на каждом томе создается максимум 64 копии.

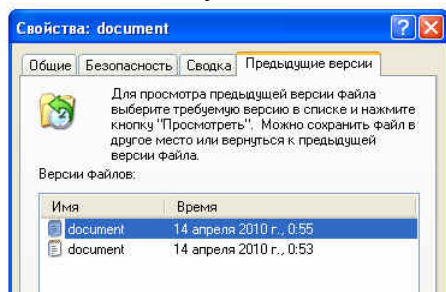
4. Настройте размер пространства для хранения копий в размере 200МБ и расписание создания теневых копий — дважды в день в 14-00 и 24-00.

5. На клиентской машине откройте файл *document.txt* и добавьте новую строку «22222».

6. На сервере вручную создайте еще одну теневую копию данного тома.

7. На клиентской машине откройте файл *document.txt* и добавьте новую строку «33333».

Использование теневых копий. После создания теневых копий пользователю становятся доступны Предыдущие версии файлов. Для использования этих возможностей нужна клиентская часть для доступа к теневым копиям. В системе Windows 2003 клиентская часть уже имеется в системе, а для Windows 2000/XP ее нужно установить. Дистрибутив клиента теневых копий хранится на сервере в папке «%SystemRoot%\system32\clients\twclient», в файле twcli32.msi. При установленном клиенте в свойствах файла, открываемого из сетевых папок, становится доступна закладка «Предыдущие версии». Проверьте, доступна ли данная закладка в Вашей клиентской системе, если нет, то установите необходимое ПО.



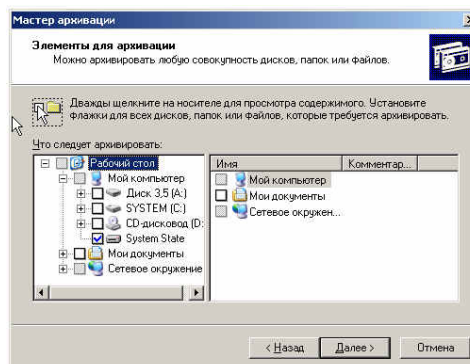
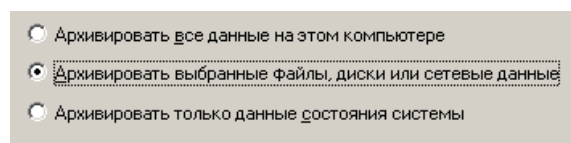
Пользователь теперь может просмотреть предыдущие копии, скопировать их в другой файл или восстановить содержимое файла в одно из предыдущих состояний. Закладка «Предыдущие версии» доступна в Свойствах не только конкретного файла, но и всей сетевой папки. Поэтому можно восстановить не только измененные файлы, но и ошибочно удаленные.

Архивирование и восстановление состояния системы

Большую часть работ по резервному копированию составляют задания на копирование бизнес-информации. Но имеется также возможность создания резервных копий для восстановления функционирования самой операционной системы. Есть два варианта архивирования системных данных — архивирование состояния системы (*System State*) и создания набора для автоматического восстановления системы после аварии (*Automated System Recovery*).

Архивирование и восстановление состояния системы

Для создания резервной копии состояния системы необходимо в утилите резервного копирования *ntbackup* при создании задания на архивирования отметить галочкой пункт *System State*:



При этом будут архивироваться следующие данные:

- системный реестр;
- база данных зарегистрированных классов объектов (*Class Registration*);
- системные загрузочные файлы;
- база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);
- база данных *Active Directory* и папка *SYSVOL* (на контроллерах доменов).

Для архивирования состояния системы, а также для последующего восстановления, обязательно нужны права администратора данного компьютера. Восстановление *Active Directory* необходимо выполнять только при загрузке системы в режиме восстановления служб каталогов (запуск меню выбора режимы загрузки операционной системы выбираются в начальный момент загрузки нажатием клавиши F8).

Автоматическое аварийное восстановление системы

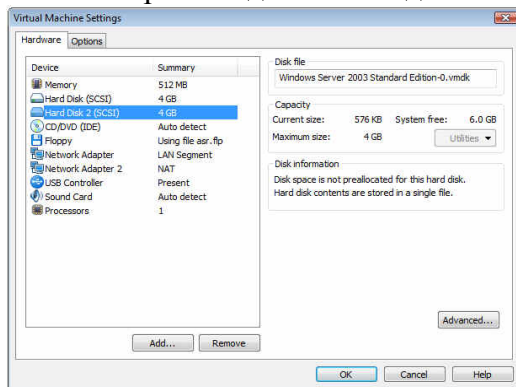
В отличие от резервного копирования состояния системы, при котором сохраняется только часть файлов операционной системы, резервное копирования для автоматического аварийного восстановления системы (*ASR, Automated System Recover*) архивирует больший объем информации — практически весь том, на котором установлена операционная система. И процедура восстановления системы становится более сложной.

▪ **Создание ASR-копии**

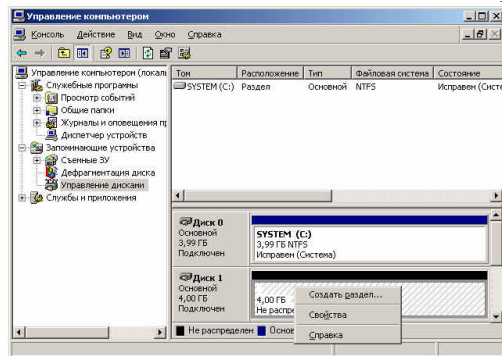
На данном этапе потребуется носитель для создания резервной копии системного тома (порядка нескольких гигабайт), причем в случае восстановления системы этот носитель должен быть доступен мастеру установки операционной системы (т.е. это либо ленточный накопитель с драйверами для контроллера и накопителя, либо дисковый накопитель с соответствующими драйверами), а также чистая отформатированная дискета для сохранения информации о конфигурации резервной копии.

1. Выберем вариант хранения данных на дополнительном дисковом накопителе. Для этого выполним следующие действия:

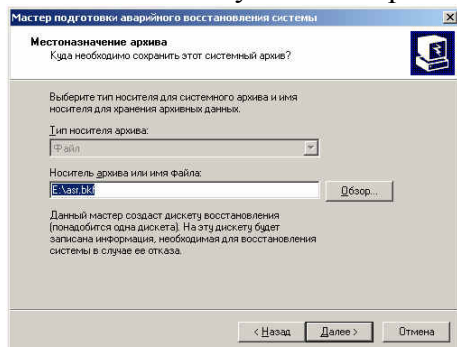
- Завершим работу нашего сервера;
- В настройках данной ОС добавим новый SCSI-винчестер объемом 4Gb;



- Запустим ОС.
- Нажмем правой клавишей мыши на «Мой компьютер» и вызываем «Управление»;
- В управлении дисками инициализируем новый диск;
- Создаем на нем основной NTFS раздел по всему объему диска.

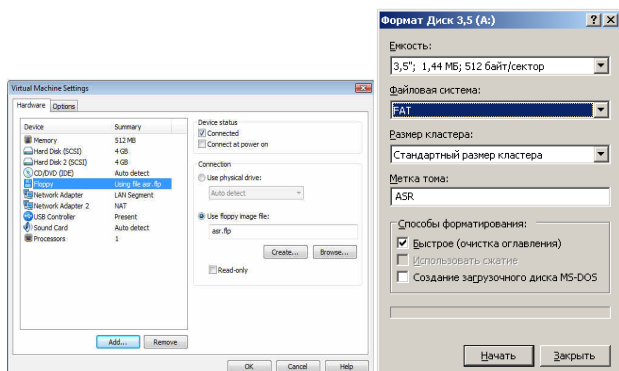


1. Запустим утилиту резервного копирования *ntbackup*.
2. Запустим «Мастер аварийного восстановления системы».
3. Укажем путь для сохранения архива.



4. Нажмем кнопку «Готово». Утилита резервного копирования начнет создание резервной ASR-копии, в нужный момент будет сделан запрос вставить чистую дискету.

Работа с дисководом в VMware имеет определенную специфику. Будем использовать виртуальную дискету. Для этого в свойствах ОС сервера в VMware выберем дискету, выберем «Использовать образ дискеты» и нажмем «Создать». Перед использованием дискеты отформатируйте ее.



После записи конфигурации резервной копии утилита попросит пометить дискету соответствующей информацией (название резервной копии и дата создания).

- **Восстановление системы с помощью ASR-копии**

1. Подготовим все необходимое для аварийного восстановления системы: установочный CD с дистрибутивом операционной системы, носитель с резервной копией, дискету с конфигурацией ASR-копии.

1. Запустим процесс установки операционной системы с загрузочного компакт-диска для этого в BIOSе виртуальной машины сервера установим загрузку с CD;

2. На первой странице мастера установки системы (после появления синего экрана) нажать клавишу F2 для запуска процесса аварийного восстановления.

3. Далее мастер установки системы выполнит новую установку системы с форматированием системного тома.

4. После выполнения установки операционной системы автоматически запустится утилита резервного копирования, и система попросит вас указать путь к резервной копии для аварийного восстановления и вставить дискету с конфигурацией ASR-копии. Будет выполнено восстановление системы из аварийной резервной копии.

5. После завершения процесса восстановления будет воссоздан работоспособный сервер в той конфигурации, которая была до аварии (при условии, конечно, что, кроме самой системы, будут также восстановлены и данные, необходимые для работы сервера).

6. В BIOSе виртуальной машины сервера установим загрузку с HDD;

Корпорация Microsoft рекомендует использовать данный метод восстановления для серверов, выполняющих особые функции, которые трудно восстановить простой переустановкой и восстановлением данных. Если сервер не исполняет какие-либо особые роли, то Microsoft рекомендует на таких серверах архивировать только данные, а в случае аварии заново переустановить сервер, снова включить его в домен и восстановить данные из резервных копий.

Контрольные вопросы:

1. Какие причины резервирования данных?
1. Какие существуют типы резервного копирования?
2. Какие преимущества дает механизм теневых копий?
3. Какие типы резервного копирования Вы знаете? В чем их особенности?
4. Кто планирует какие данные нужно резервировать?
5. Какие недостатки имеет архивирование, сделанное в данной лабораторной работе?
6. Какие данные необходимо резервировать?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 37

Работа с удаленными файлами при помощи FTP. Использование SMTP

Цель работы: Изучить основы удаленного управления в Linux Ubuntu.

Оснащение: МУ к ПЗ

Теоретическая часть

Настройка ftp-сервера

FTP (англ. File Transfer Protocol - протокол передачи файлов) - протокол, предназначенный для передачи файлов в сетях передачи данных. FTP позволяет подключаться к серверам FTP, просматривать содержимое каталогов и загружать файлы с сервера или на сервер; кроме того, возможен режим передачи файлов между серверами.

FTP является одним из старейших прикладных протоколов, появившимся задолго до HTTP, в 1971 году. Он и сегодня широко используется для распространения программного обеспечения и доступа к удалённым хостам.

Протокол FTP относится к протоколам прикладного уровня и для передачи данных использует транспортный протокол TCP. Команды и данные, в отличие от большинства других протоколов, передаются по разным портам. Исходящий порт 20, открываемый на стороне сервера, используется для передачи данных, порт 21 для передачи команд. Порт для приема данных клиентом определяется в диалоге согласования. В случае, если передача файла была прервана по каким-либо причинам, протокол предусматривает средства для докачки файла, что бывает очень удобно при передаче больших файлов.

Vsftpd (Very Secure FTP Daemon или Очень Защищенный FTP Демон) является одним из самых простых в конфигурировании и наиболее часто используемым FTP сервером. Vsftpd обслуживает ftp серверы debian, redhat, ubuntu и прочих крупных компаний. Благодаря предельной простоте настройки, поднятие ftp сервера с помощью vsftpd редко занимает более 5 - 10 минут.

В данной лабораторной работе предполагается показать принцип создания файлового сервера, на который все пользователи смогут складывать файлы, удалять их, создавать директории и т.д.

Установка vsftpd

Установка vsftpd приведена на рис. 4.1. Перед установкой необходимо проверить, что есть соединение с Internet.

```
work@work:~$ sudo apt-get install vsftpd
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 4.1. Установка ftp

Настройка vsftpd

Конфигурирование vsftpd осуществляется редактированием файла /etc/vsftpd.conf (Рис. 4.2). Комментариев (при минимальном знании английского) обычно достаточно, чтобы разобраться что к чему:

- anon_root - директория для анонимных пользователей (/var/ftp/ по умолчанию в большинстве дистрибутивов);
- anonymous_enable - разрешить доступ анонимным пользователям;
- local_enable - разрешить доступ локальным пользователям;
- write_enable - разрешить запись;
- anon_upload_enable - разрешить запись анонимным пользователям

Таким образом, можно отредактировать эти записи в конфиге следующим образом (не стоит удалять остальные опции, если вы не знаете, что они делают):

```
#возможность работы в автономном режиме
```

```
listen=YES
```

```
#позволяем анонимных пользователей, учетки anonymous и ftp являются синонимами
```

```
anonymous_enable=YES
```

```
#разрешаем локальных пользователей (локальные пользователи - это те, которые
```

```
#зарегистрированы в системе, то есть на них есть учетные записи)
```

```

local_enable=YES
#разрешаем любые формы записи на FTP сервер
write_enable=YES
#разрешаем анонимным пользователям upload
anon_upload_enable=YES
#разрешаем анонимным пользователям создавать директории
anon_mkdir_write_enable=YES
#разрешаем анонимным пользователям переименовывать файлы
anon_other_write_enable=YES
#у анонимов пароль спрашивать не будем
no_anon_password=YES
#директория для доступа анонимных пользователей (если пользователь
присутствует)
anon_root=/home/ftp/
#разрешаем соединение по 20 порту
connect_from_port_20=YES
#поддержка древних FTP клиентов
async_abor_enable=YES
#используем родное время, а не GMT
use_localtime=YES
#небольшое приветствие
ftpd_banner=Hello! We come in peace!
#возможность работы как фоновый процесс
background=YES
# Должны ли пользователи находится только в своих директориях
YES/NO chroot_local_user=YES

```

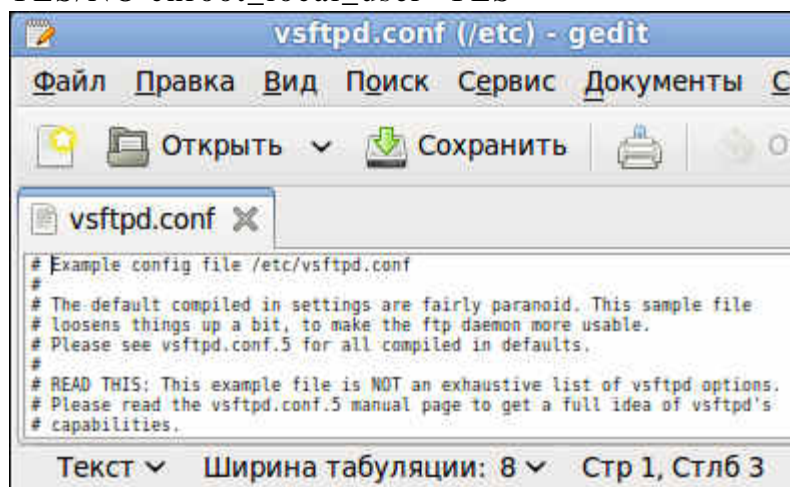


Рис. 4.2. Файл конфигурации ftp

Telnet

TELNET (англ. TErминаL NETwork) - сетевой протокол для реализации текстового интерфейса по сети (в современной форме - при помощи транспорта TCP). Название «telnet» имеют также некоторые утилиты, реализующие клиентскую часть протокола. Современный стандарт протокола описан в RFC 854.

Выполняет функции протокола прикладного уровня модели OSI.

Назначение протокола TELNET в предоставлении достаточно общего, двунаправленного, восьмибитного байт-ориентированного средства связи. Его основная задача заключается в том, чтобы позволить терминальным устройствам и терминальным процессам взаимодействовать друг с другом. Предполагается, что этот протокол может быть использован для связи вида терминал-терминал («связывание») или для связи процесс-процесс («распределенные вычисления»).

В протоколе не предусмотрено использование ни шифрования, ни проверки подлинности данных. Поэтому он уязвим для любого вида атак, к которым уязвим его транспорт, то есть протокол TCP. Для функциональности удалённого доступа к системе в настоящее время применяется сетевой

протокол SSH (особенно его версия 2), при создании которого упор делался именно на вопросы безопасности. Так что следует иметь в виду, что сессия Telnet весьма незащищена, если только не осуществляется в полностью контролируемой сети или с применением защиты на сетевом уровне (различные реализации виртуальных частных сетей). По причине ненадёжности от Telnet как средства управления операционными системами давно отказались.

Сетевой протокол ssh

SSH - это специальный сетевой протокол, позволяющий получать удаленный доступ к компьютеру с большой степенью безопасности соединения.

В основном, ssh реализован в виде двух приложений – ssh-сервера и ssh-клиента. В Ubuntu используется свободная реализация клиента и сервера ssh - OpenSSH. При подключении клиент проходит процедуру авторизации у сервера и между ними устанавливается зашифрованное соединение. OpenSSH сервер может работать как с протоколом ssh1, так и с протоколом ssh2. В настоящее время протокол ssh1 считается небезопасным, поэтому его использование крайне не рекомендуется.

Установить OpenSSH можно так:

```
work@work:~$ sudo aptitude install ssh
```

Рис. 4.3. Установка OpenSSH

Метапакет ssh содержит в себе и клиент и сервер, при этом скорее всего будет установлен только сервер, т. к. клиент часто бывает установлен в Ubuntu по умолчанию.

SSH сервер автоматически прописывается в автозагрузку при установке. Управлять его запуском/остановкой или перезапуском можно при помощи команд:

```
sudo service ssh stop|start|restart
```

Основным файлом конфигурации ssh-сервера является файл /etc/ssh/sshd_config, который должен быть доступным для чтения/редактирования только суперпользователю. После каждого изменения этого файла необходимо перезапустить ssh-сервер для применения изменений.

Сам по себе, неправильно настроенный ssh сервер - огромная уязвимость в безопасности системы, т. к. у возможного злоумышленника есть возможность получить практически неограниченный доступ к системе. Помимо этого, у sshd есть много дополнительных полезных опций, которые желательно включить для повышения удобства работы и безопасности.

Для правильной настройки ssh с точки зрения безопасности необходимо отредактировать всего семь параметров:

1. PermitRootLogin – отключение возможности авторизации под суперпользователем;
1. AllowUsers, AllowGroups - предоставление доступа только указанным пользователям или группам;
2. DenyUsers, DenyGroups - блокировка доступа определенным пользователям или группам;
3. Port - изменение порта SSHD;
4. LoginGraceTime - изменение времени ожидания авторизации;
5. ListenAddress - ограничение авторизации по интерфейсу;
6. ClientAliveInterval - рассоединение при отсутствии активности в шелле.

Сменить стандартный порт (22) на котором слушает sshd. Это связано с тем, что многочисленные сетевые сканеры постоянно пытаются соединиться с 22-м портом и как минимум получить доступ путем перебора логинов/паролей из своей базы. Даже если у вас и отключена парольная аутентификация - эти попытки сильно засоряют журналы и (в большом количестве) могут негативно повлиять на скорость работы ssh-сервера. Если же вы по какой либо причине не желаете изменить стандартный порт вы можете использовать как различные внешние утилиты для борьбы брутфорсерами, например fail2ban, так и встроенные, такие как MaxStartups.

По умолчанию root-доступ разрешен. Это означает, что клиент при подключении в качестве пользователя может указать root, и во многих случаях получить контроль над системой. При условии, что по умолчанию в Ubuntu пользователь, добавленный при установке системы имеет возможность решать все административные задачи через sudo, создавать возможность root доступа к системе как минимум странно. Рекомендуется отключить эту опцию совсем.

```
*sshd_config X
Protocol 2
AddressFamily inet
PasswordAuthentication no
SendEnv LANG LC *
HashKnownHosts yes
GSSAPIAuthentication yes
GSSAPIDelegateCredentials no
PermitRootLogin no
AllowUser work
Port 2002
LoginGraceTime 1m
ClientAliveInterval 600
ClientAliveCountMax 0
```

Рис. 4.4. Файл конфигурации ssh

Разрешенная по умолчанию парольная аутентификация является практически самым примитивным способом авторизации в ssh. С одной стороны это упрощает конфигурацию и подключение новых пользователей (пользователю достаточно знать свой системный логин/пароль), с другой стороны пароль всегда можно подобрать, а пользователи часто пренебрегают созданием сложных и длинных паролей. Специальные боты постоянно сканируют доступные из интернета ssh сервера и пытаются авторизоваться на них путем перебора логинов/паролей из своей базы. Настоятельно не рекомендуется использовать парольную аутентификацию.

Как уже было сказано, ssh может работать с протоколами ssh1 и ssh2. При этом использование небезопасного ssh1 крайне не рекомендуется.

В конечном итоге файл конфигурации должен выглядеть так, как на рис. 4.4.

Для удаленного доступа с операционной системы Windows необходимо установить на ней специальный клиент – putty (рис 4.5).

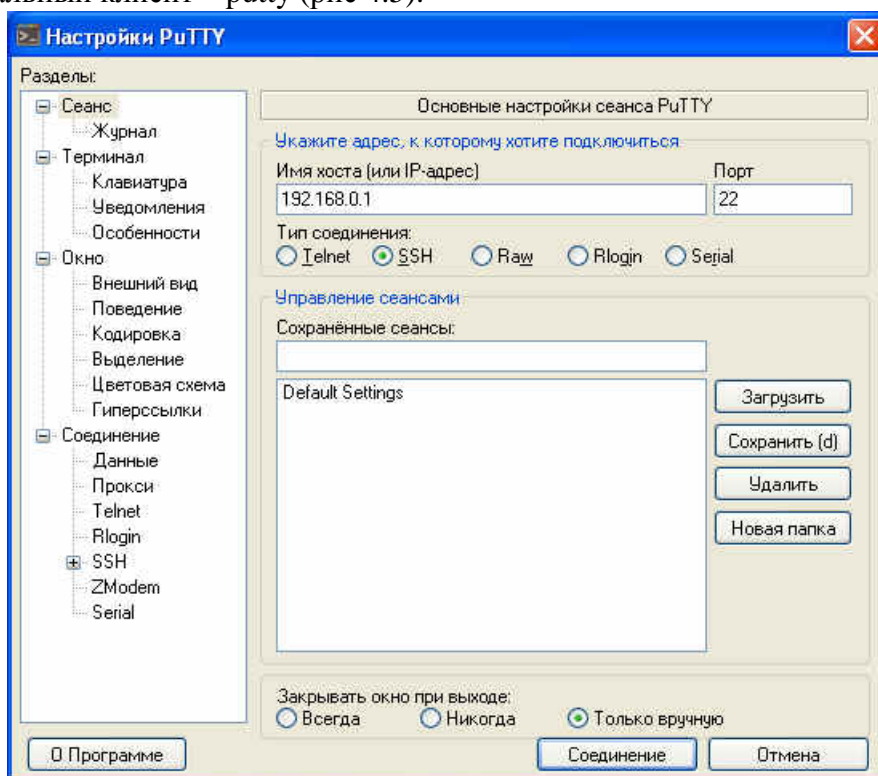


Рис. 4.5. PuTTY

Для настройки сессии введите IP хоста (192.168.0.1). Так же настройте кодировку в пункте Translation, поменяв её на UTF-8.

Веб-сервер

Apache HTTP-сервер – свободный веб-сервер. Apache является кроссплатформенным программным обеспечением, поддерживает операционные системы Linux, BSD, Mac OS, Microsoft Windows, Novell NetWare, BeOS.

Основными достоинствами Apache считаются надёжность и гибкость конфигурации. Он позволяет подключать внешние модули для предоставления данных, использовать СУБД для аутентификации пользователей, модифицировать сообщения об ошибках и т. д. Поддерживает IPv6.

Для установки apache2 введите команду, представленную на рис. 4.6.

```
work@work:~$ sudo apt-get install apache2
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
```

Рис. 4.6. Установка apache2

Файлы конфигурации Apache2 находятся в директории: /etc/apache2:

- conf.d/
- sites-available/
- sites-enabled/
- mods-available/
- mods-enabled/
- apache2.conf
- envvars
- httpd.conf
- ports.conf

В Ubuntu основным файлом настройки Apache2 является apache2.conf. Он играет роль системного файла, в котором собраны основные и самые важные настройки сервера.

Файл httpd.conf - пустой и предназначен для добавления дополнительных настроек, он включен в основной файл настройки apache2.conf

В файле envvars описаны переменные среды, необходимые для функционирования Apache-сервера.

В ports.conf вынесены настройки портов на которые можно будет подключиться к серверу или конкретному сайту на нем.

В папке conf.d находятся дополнительные конфигурационные файлы.

Для описания всех доступных сайтов используется папка sites-available в которой расположены файлы с описанием виртуальных хостов - VirtualHosts, опубликованные же сайты находятся в папке sites-enabled в виде ссылок на файлы доступных сайтов из папки sites-available.

Таким же образом в папках mods-available и mods-enabled настраивается доступность модулей используемых сервером.

Теперь необходимо подготовить компьютер к работе веб-сервера. Прежде всего необходимо создать единую папку для всех сайтов, которые будут там размещаться, например /home/user/www. Лучшее место для такой папки это домашний каталог пользователя. Далее в этой папке необходимо создать папку сайта. Например, /home/user/www/site1. И в эту папку кинуть файлы сайта.

Следующая команда (рис. 4.7) создает запись виртуального хостинга копируя стандартную запись из файла конфигурирования Apache:

```
work@work:~$ sudo cp /etc/apache2/sites-available/default /etc/apache2/sites-enabled/site1
```

Рис. 4.7. Копирование файла конфигурации

Теперь необходимо отредактировать файл, который находится по директории /etc/apache2/sites-enabled/site1. Необходимо настроить имя сервера, URL сервера и директорию, по которой находятся файлы сайта. После настроек файл конфигурации должен выглядеть, например, так, как на рис. 4.8.

```
*site1 X
<VirtualHost *:80>
  ServerName sitel
  ServerAlias sitel.my www.sitel.my
  DocumentRoot /home/work/www/sitel
</VirtualHost>
```

Рис. 4.8. Файл конфигурации сайта site1

Теперь необходимо как-то научить операционную систему распознавать домен .my. Для этого достаточно прописать необходимые строки в файле /etc/hosts, например так, как на рис. 4.9.

```
*host X
127.0.0.1 localhost
127.0.1.1 work
127.0.1.2 sitel.my www.sitel.my
```

Рис. 4.9. Редактирование файла hosts

Для начала необходимо разместить ссылку на VirtualHost в папку sites-enabled, и перечитать конфигурацию сервера Apache. Для создания ссылки можно выполнить такую команду и перечитать параметры (рис. 4.10). После этого ваш сайт, файлы которого размещаются в директории /home/user/www/site1 будет отображаться в браузере по адресу: site1.my или www.site1.my.

```
work@work:~$ sudo a2ensite site1
Site site1 already enabled
work@work:~$ sudo /etc/init.d/apache2 reload
 * Reloading web server config apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.1.1 for ServerName
[ OK ]
```

Рис. 4.10. Активация сайта

Практическая работа

1. На виртуальной машине разверните ftp-сервер;
1. Разрешите анонимный доступ для всех пользователей на данный ftp-сервер. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
2. Настройте разграничение прав доступа к определенным каталогам пользователей на ftp-сервере. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
3. Настройте смешанный режим доступа анонимных и зарегистрированных пользователей. Проверьте работу ftp-сервера с данной конфигурацией с вашей основной операционной системы;
4. Установить ssh-сервер на вашу операционную систему Linux. Настройте ssh с точки зрения безопасности;
5. На вашей основной операционной системе установить ssh-клиент (если основная операционная система Linux) или putty (если основная операционная система Windows). Проверьте работу ssh, настроив клиент соответствующим образом;
6. Установить веб сервер на Linux Ubuntu;
7. Создайте простую html-страничку. Разместите её на веб-сервере по веб-адресам: work.my и www.work.my.

Контрольные вопросы

1. Каково назначение ftp-сервера?
1. Каким образом производится настройка vsftpd?
2. Каково назначение сетевого протокола SSH?
3. Какие основные параметры рекомендуется менять при настройке SSH с точки зрения его безопасности и почему?
4. Каково назначение Telnet? Почему Telnet не рекомендуется использовать?
5. Каково назначение Apache?
6. Какие основные конфигурационные файлы Apache существуют?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 38 Работа с сетью в среде ОС Linux

Цель работы: Научится управлять сетевыми подключениями в ОС Linux.

Оснащение: МУ к ПЗ

Теоретическая часть

В ОС Linux присутствуют следующие файлы конфигурации сети вне зависимости от версии дистрибутива:

–/etc/hosts - в этом файле можно прописать IP-адреса и имена узлов локальной сети, но обычно здесь указывается только IP-адрес узла localhost (127.0.0.1), потому что сейчас даже в небольшой локальной сети устанавливается собственный DNS-сервер;

–/etc/hosts.allow – содержит IP-адреса узлов, которым разрешен доступ к сервисам данного узла;

–/etc/hosts.deny – содержит IP-адреса узлов, которым запрещен доступ к сервисам данного узла;

–/etc/iftab – содержит таблицу интерфейсов, т. е. соответствие имен интерфейсов и их MAC-адресов;

–/etc/motd – файл задает сообщение дня (Message of the day). Данный файл используется многими сетевыми сервисами, например, FTP-, SSH-серверами, которые при регистрации пользователя могут выводить сообщение из этого файла;

–/etc/resolv.conf – задает IP-адреса серверов DNS;

–/etc/services – база данных сервисов, задающая соответствие символического имени сервиса (например, pop3) и номера порта (110/tcp, tcp - это наименование протокола).

Прежде чем начать работу, убедитесь, что драйвер сетевого устройства корректно установлен, кабель (при проводном соединении) исправен и подсоединен.

Команда

```
$ sudo lshw -C network
```

позволяет посмотреть подключенные сетевые устройства. Пример вывода команды (рис. 3.1):

```
work@work:~$ sudo lshw -c network
*-network:0
   description: Ethernet interface
   product: 82540EM Gigabit Ethernet Controller
   vendor: Intel Corporation
   physical id: 3
   bus info: pci@0000:00:03.0
   logical name: eth0
   version: 02
   serial: 08:00:27:61:28:dc
   size: 1GB/s
   capacity: 1GB/s
   width: 32 bits
   clock: 66MHz
   capabilities: pm pci_x bus_master cap_list ethernet phy
   sical tp 10bt 10bt-fd 100bt 100bt-fd 1000bt-fd autonegotiat
   ion
   configuration: autonegotiation=on broadcast=yes driver=
   e1000 driverversion=7.3.21-k5-NAPI duplex=full firmware=N/
   A ip=10.0.2.15 latency=64 link=yes mingnt=255 multicast=yes
   port=twisted pair speed=1GB/s
   resources: irq:19 memory:f0000000-f001ffff ioport:d01
   0(size=8)
```

Рис. 3.1. Просмотр подключенных сетевых устройств

При выводе информации вы можете увидеть следующие свойства устройства: description – тип устройства, product – название адаптера, vendor - производитель устройства, logical name - имя сетевого интерфейса, serial- физический адрес устройства (mac-адрес), driver - используемый драйвер, driverversion - версия драйвера, link - наличие ссылки, speed - текущая скорость подключения.

Обратите внимание на имя сетевого интерфейса - eth0. Это имя будет далее применяться для настройки именно данной сетевой карты. Где eth обозначает что используется Ethernet интерфейс, а 0

- номер устройства. Если у вас установлено несколько сетевых устройств то соответственно им будет присвоено имена: eth0, eth1, eth2 и т.д.

Различные сетевые утилиты, предназначенные для автоматического конфигурирования сети должны быть выключены. Для отключения запущенного Network Manager введите команду, представленную на рис. 3.2.

```
work@work:~$ sudo /etc/init.d/network-manager stop
Rather than invoking init scripts through /etc/init.d,
use the service(8)
utility, e.g. service network-manager stop

Since the script you are attempting to invoke has been
converted to an
Upstart job, you may also use the stop(8) utility, e.g.
stop network-manager
```

Рис. 3.2. Остановка NetworkManager

Network Manager после этого не выгрузится, но не будет видеть никаких соединений.

Отключение автоматического запуска Network Manager:

1. Откройте для редактирования файл /etc/rc.local, например командой:

```
$ sudo gedit /etc/rc.local
```

2. Добавьте в него (перед строкой со словом exit 0) выключение NM (рис. 3.3):

```
rc.local X
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
/etc/init.d/network-manager stop
exit 0
```

Рис. 3.3. Редактирование файла rc.local

Настройка проводной сети

Для настройки IP адреса, шлюза по умолчанию, маски подсети, отредактируйте файл конфигурации /etc/network/interfaces, например так:

```
$ sudo gedit /etc/network/interfaces
```

Для статического IP отредактируйте данный файл так, как представлено на рис. 3.4:

```
*interfaces X
auto lo
iface lo inet loopback
iface eth0 inet static
address 192.168.0.1
netmask 255.255.255.0
gateway 192.168.0.254
auto eth0
```

Рис. 3.4. Настройка сетевого интерфейса

Где:

- iface eth0 inet static - указывает, что интерфейс (iface eth0) находится в диапазоне адресов IPv4 (inet) со статическим ip (static);
- address 192.168.0.1 - указывает что IP адрес (address) нашей сетевой карты 192.168.0.1;
- netmask 255.255.255.0 - указывает что маска подсети (netmask) имеет значение 255.255.255.0;
- gateway 192.168.0.254 - адрес шлюза (gateway) по умолчанию 192.168.0.254;
- auto eth0 - указывает системе что интерфейс eth0 необходимо включать автоматически при загрузке системы с вышеуказанными параметрами.

eth0 - имя подключаемого своего интерфейса. Список интерфейсов можно посмотреть набрав (рис. 3.5):


```
$ ifconfig -a
```

```
work@work:~$ ifconfig -a
eth2      Link encap:Ethernet  HWaddr 08:00:27:e8:d3:74
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:76 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1770 (1.7 KB)  TX bytes:13316 (13.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5936 (5.9 KB)  TX bytes:5936 (5.9 KB)
```

Рис. 3.5. Вывод списка интерфейсов

Пример конфигурации для динамического IP приведен на рис. 3.6:

```
*interfaces X
auto lo
iface lo inet loopback
iface eth0 inet dhcp
auto eth0
```

Рис. 3.6. Конфигурация для динамического IP

Временная настройка IP адреса и маски подсети

При необходимости задать пробные настройки, выполните (рис. 3.7):

```
work@work:~$ sudo ifconfig eth0 192.168.0.1 netmask
255.255.255.0 up
```

Рис. 3.7. Временные настройки адаптера

Где 192.168.0.1 - IP адрес, 255.255.255.0 - маска подсети. eth0 - подключаемый сетевой интерфейс.

Данные настройки пропадут после перезагрузки системы и не повлияют на файл /etc/network/interfaces.

Межсетевой экран

Ядро linux содержит подсистему (модуль) Netfilter, которая используется для управления входящими или проходящими через сервер пакетами. Все современные брандмауэры используют эту систему для фильтрации tcp пакетов. Без интерфейса эта система мала полезна для администратора. Для управления используется iptables. При получении пакета вашим сервером, он передается Netfilter для принятия им решения: принять, обработать, или отбросить его. Таким образом, iptables это все, что нужно для управления брандмауэром. Для управления iptable существует множество программ, в том числе и ufw, которая в Ubuntu используется по умолчанию.

Ufw представляет из себя простой механизм для создания правил фильтрации пакетов IPv4 и IPv6. Данный пакет, после установки, по умолчанию отключен. Для включения ufw необходимо ввести команду:

```
work@work:~$ sudo ufw enable
Межсетевой экран активен и будет запущен при запуске системы
```

Рис. 3.8. Команда включение ufw

После запуска межсетевого экрана необходимо открыть все необходимые порты. Это делается командой, приведенной на рис. 3.9.

```
work@work:~$ sudo ufw allow 22
Правило добавлено
```

Рис. 3.9. Открытие порта

В данном примере межсетевой экран открывает 22 порт, который используется ssh. Для того, что бы закрыть открытый порт, необходимо ввести команду, приведенную на рис. 3.10.

```
work@work:~$ sudo ufw deny 22
Правило обновлено
```

Рис. 3.10. Закрытие порта

При вводе данной команды, мы получили сообщение, что правило обновлено. Так же какое-либо правило можно удалить, для этого необходимо воспользоваться командой (рис.3.11):

```
work@work:~$ sudo ufw delete deny 22
Правило удалено
```

Рис. 3.11. Удаление правила

Возможно разрешить доступ для определенных хостов или сетей. На рис. 3.12 показано как разрешить доступ хосту с ip адресом 192.168.0.2 на хост с любым ip по протоколу ssh. Если заменить 192.168.0.2 на 192.168.0.0/24 то мы разрешим протокол ssh для любого хоста этой локальной сети.

```
work@work:~$ sudo ufw allow proto tcp from 192.
168.0.2 to any port 22
Правило добавлено
work@work:~$ sudo ufw allow proto tcp from 192.
168.0.0/24 to any port 22
Правило добавлено
```

Рис. 3.12. Определение доступа для определенных хостов

При указании опции --dry-run будет выводить результат применения правила, но применяться они не будут. Например, если набрать команду:

```
sudo ufw --dry-run allow http
```

будет показана цепочка применяемых правил для открытия порта HTTP.

Для отключения ufw, просмотра состояния брандмауэра и вывода дополнительной информации о нем, необходимо воспользоваться соответствующими командами, приведенными на рис. 3.13.

```
work@work:~$ sudo ufw disable
Фаервол остановлен и деактивирован при загрузке
work@work:~$ sudo ufw status
Состояние: неактивен
work@work:~$ sudo ufw status verbose
Состояние: неактивен
```

Рис. 3.13. Команды остановки и просмотра состояния ufw

Если порт который вы хотите открыть или закрыть определен в файле /etc/services, вы можете указывать текстовое имя порта вместо его номера. Например, в приведенных выше примерах, можно заменить 22 на ssh.

Практическая работа

1. Выведет на экран все подключенные сетевые интерфейсы;
1. Отключите Network Manager, и отключите автоматический запуск Network Manager'a;
2. Настройте свой адаптер, задав следующие параметры:
IP: 192.168.0.1
Маска сети: 255.255.255.0
3. Включите межсетевой экран и добавьте в него правило: запретить входящий трафик по 80му порту;
4. Запретите любой исходящий трафик по 20му порту;
5. Разрешить доступ по 20му порту с ip-адреса 192.168.0.1.

Контрольные вопросы

1. Какие файлы конфигурации сети существуют в Linux?
1. Каким образом присваиваются имена интерфейсам в Linux?
2. Какого назначение модуля Ufw?
3. Каким образом осуществляется фильтрация пакетов в Linux?

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 39 Web-браузер. Интернет и его службы

Цель:

1. Научить определять *IP-адрес* компьютера.
2. Ознакомиться с назначением и возможностями *Web-браузера Internet Explorer*.
3. Сформировать навыки работы с программой *Internet Explorer*.
4. Научить проводить поиск и «скачивания» информации в сети.
5. Сформировать навыки работы с поисковыми системами.
6. Получить основные навыки работы с электронной почтой.

Оснащение: МУ к ПЗ

Краткие теоретические сведения

Средства просмотра Web-страниц

Документы *Интернета*, предназначенные для отображения в электронной форме, можно просмотреть с помощью *Web-браузера*, установленного на компьютере пользователя. *Браузер (browser)* — программа для отображения и работы с гипертекстовыми документами.

Основные функции браузеров:

- установление связи с *Web-сервером*, на котором хранится документ, и загрузка всех компонентов комбинированного документа;
- интерпретация тегов языка *HTML*, форматирование и отображение *Web-страницы* в соответствии с возможностями компьютера, на котором браузер работает;
- предоставление средств для отображения мультимедийных и других объектов, входящих в состав *Web-страниц*, а также механизма расширения, позволяющего настраивать программу на работу с новыми типами объектов;
- обеспечение автоматизации поиска *Web-страниц* и упрощение доступа к *Web-страницам*.
- предоставление доступа к встроенным или автономным средствам для работы с другими службами *Интернета*.

В настоящее время существует достаточное количество *Web-браузеров*. Наиболее известными являются *Internet Explorer*, *Netscape Navigator*, *Opera*, *No Trax* и др.

Основные функции программы Internet Explorer:

- предоставляет единый метод доступа к локальным документам компьютера и к информации, доступной в *Интернете*;
- обеспечивает работу с *World Wide Web*;
- предоставляет идентичные средства работы с локальными папками компьютера и файловыми архивами *FTP*;
- дает доступ к средствам связи через *Интернет*.

Существуют различные способы запуска программы Internet Explorer:

- с помощью значка *Internet Explorer* на *Рабочем столе* или на *Панели быстрого запуска*;
- с помощью *Главное меню ОС Windows: Пуск → Программы → Internet Explorer*.

Открытие и просмотр Web-страниц

Открыть Web-страницу можно:

- введя *URL-адрес Web-страницы* в поле панели *Адрес*, и щелкнув на кнопке *Переход*.
- выбрав *URL-адрес Web-страницы* в раскрывающемся списке панели *Адрес*, и щелкнув на кнопке *Переход*.

Открытая *Web-страница* отображается в рабочей области окна обозревателя. По умолчанию воспроизводится все ее содержимое, включая графические иллюстрации и встроенные мультимедийные объекты.

Управление просмотром осуществляется при помощи управляющего меню, панелей инструментов, а также активных элементов, имеющих в открытом документе, например *гиперссылок*.

Работа с гиперссылками

Навигация по *Internet* чаще выполняется с помощью *гиперссылок*. При отображении *Web-страницы* гиперссылки выделяются цветом (обычно синим) и подчеркиванием. При наведении на нее указателя мыши он принимает форму кисти руки с вытянутым указательным пальцем, а сама гиперссылка при соответствующей настройке браузера изменяет цвет.

Адрес *URL*, на который указывает ссылка, отображается в строке состояния. При щелчке на гиперссылке соответствующая *Web-страница* загружается вместо текущей. Если гиперссылка указывает на произвольный файл, его загрузка происходит по протоколу *FTP*.

Гиперссылки бывают: текстовые, графические (представленные рисунком) и изображения-карты, объединяющие несколько ссылок в рамках одного изображения. Для просмотра ссылок на открытой *Web-странице* удобно использовать клавишу *TAB*. При ее нажатии фокус ввода (пунктирная рамка) перемещается к следующей ссылке. Перейти по ссылке можно, нажав клавишу *ENTER*. При таком подходе последовательно перебираются текстовые и графические ссылки, а также отдельные области изображений-карт.

Дополнительные возможности использования гиперссылок предоставляет их контекстное меню. Чтобы открыть новую страницу, не закрывая текущей, применяют команду *Открыть в новом окне*. В результате открывается новое окно браузера.

Разные операции, относящиеся к текущей странице и ее элементам, удобно осуществлять через контекстное меню. Так, например, рисунок, имеющийся на странице, можно:

- сохранить как файл (*Сохранить рисунок как*);
- использовать как фоновый рисунок (*Сделать рисунком рабочего стола*) или как активный элемент (*Сохранить как элемент рабочего стола*).

Если рисунок выполняет функции графической ссылки, к нему можно применять как команды, относящиеся к изображению, так и команды, относящиеся к ссылке.

Приемы управления Internet Explorer

Кнопки панели инструментов:

- *Назад* – возврат к странице, которая просматривалась некоторое время назад.
- Присоединенная к кнопке *Назад* кнопка раскрывающегося списка – возврат на несколько страниц назад.
- *Вперед* – отмена действий, выполненных при помощи кнопки *Назад*.
- *Остановить* – остановка процесса загрузки страницы, если загрузка затянулась или не требуется.
- *Обновить* – повторная загрузка *Web-страницы*, если ее загрузка была прервана или содержание документа изменилось.
- *Домой* – загрузка «домашней» страницы.

Команды меню:

- *Файл* позволяют: создать новое окно, сохранить открытый документ на своем компьютере, распечатать его, включить или выключить режим автономной работы, а также завершить работу с программой.
- *Правка* позволяют: копировать фрагменты документа в буфер обмена, искать текст на *Web-странице*.
- *Вид* позволяют: включать/выключать отображения служебных элементов окна (панелей инструментов, дополнительных панелей, строки состояния), выбирать шрифт и кодировку символов.
- *Избранное* позволяют вести список регулярно посещаемых страниц и осуществлять быстрый доступ к ним.
- *Сервис* позволяют выполнять переход к использованию программ для работы с другими службами *Интернета*, настраивать браузер.

Настройка свойств Internet Explorer

Для эффективной и комфортной работы в *Интернете* необходима настройка браузера. Параметры оптимальной настройки зависят от многих факторов:

- свойств видеосистемы компьютера;
- производительности действующего соединения с *Интернетом*;
- содержания текущего *Web-документа*;
- личных предпочтений индивидуального пользователя.

Начать настройку программы *Internet Explorer* можно:

- из самой программы *Сервис* → *Свойства обозревателя*.
- или *Панель управления* → значок *Свойства обозревателя*.

Открывшееся диалоговое окно отличается только названием (*Свойства обозревателя* и *Свойства:Интернет*).

Окно содержит шесть вкладок для настройки разных групп параметров:

1) вкладка *Общие* позволяет:

- указать, какую страницу использовать в качестве основной;
- задать объем дискового пространства для хранения временных файлов *Интернета*;
- удалить временные файлы;
- управлять оформлением отображаемых *Web-страниц*;
- при помощи кнопки *Цвета* настраивать цвета;
- при помощи кнопки *Шрифты* настраивать шрифты;
- при помощи кнопки *Оформление* задать принудительное использование параметров форматирования: цветов (флажок *Не учитывать цвета, указанные на веб-страницах*), начертаний шрифтов (*Не учитывать шрифты, указанные на веб-страницах*) и размеров шрифтов (*Не учитывать размеры шрифтов, указанные на веб-страницах*).

2) вкладка *Подключение* позволяет:

- настраивать свойства соединения с *Internet* (доступны те же операции, что и при непосредственном использовании папки *Удаленный доступ к сети*);
- указать, какое именно соединение должно использоваться при работе браузера;
- помощью переключателей можно задать режим отказа от автоматического подключения, стандартный режим подключения при отсутствии соединения или режим использования только одного соединения.

3) вкладка *Программы* позволяет выбирать программы, используемые для работы в *Интернете*. Все виды программ, кроме календаря (для ведения списка дел, встреч, праздников и прочего), входят непосредственно в дистрибутивный пакет *Internet Explorer*.

4) вкладка *Безопасность*:

- предоставляет средства защиты от потенциально опасного содержимого *Web-документов*;
- позволяет указать *Web-узлы*, взаимодействие с которыми следует считать опасным, и запретить прием с них информации.

5) вкладка *Содержание* позволяет:

- ограничить доступ к узлам с неприемлемым содержанием;
- управлять использованием электронных сертификатов.

6) вкладка *Дополнительно* позволяет:

- управлять отображением мультимедийных объектов;
- использовать дополнительные настройки оформления;
- управлять режимом поиска *Web-страниц*, содержащих нужную информацию;
- соблюдать конфиденциальность работы с помощью средств шифрования, использования электронных сертификатов и своевременного удаления временных файлов;
- контролировать использование средств языка Java.

Запись информации с Web-страниц на диск

Запись содержания всей страницы:

1) Выполнить команду *Файл* → *Сохранить как*;

2) В поле *Имя* файла задать имя;

3) В поле *Тип* файла выбрать:

- *Веб-страница, полностью* – сохраняет страницу целиком (автоматически создается одноименная папка с файлом, в которую помещаются графические объекты страницы);

- *Веб-страница, только HTML* – сохраняет текст и форматирование страницы, для рисунков и других объектов указывается только местоположение;

- *Текстовый файл* – сохраняет только неформатированный текст;

4) Выбрать вид кодировки;

5) Нажать кнопку *Сохранить*.

Запись фрагмента страницы:

- 1) Выделить фрагмент;
- 2) Скопировать его в буфер обмена;
- 3) Запустить текстовый редактор (процессор);
- 4) Вставить фрагмент;
- 5) Сохранить обычным образом.

Запись графической картинки или анимации:

- 1) Вызвать контекстное меню объекта;
- 2) Выбрать команду *Сохранить рисунок как*;
- 3) Выбрать диск, папку, задать имя, выбрать тип файла;
- 4) Нажать кнопку *Сохранить*.

Запись рефератов, курсовых.....

Рефераты, курсовые обычно хранятся в заархивированном виде, поэтому их надо сначала скачать, а потом разархивировать и просмотреть в текстовом редакторе.

- Чтобы скачать файл надо:
- щелкнуть левой кнопкой мыши по выбранному файлу или тексту *Скачать файл*;
- нажать кнопку *Скачать*;
- выбрать диск, папку, задать имя файла (оставить предлагаемое);
- нажать кнопку *Сохранить*;
- после окончания загрузки окно закроется.

Замечание. Процесс загрузки не влияет на работу браузера, ее можно продолжать, в том числе скачивать и другие файлы.

Электронная почта

Электронная почта (*e-mail – electronic mail*) является одной из наиболее ранних информационных служб *Internet*. Она позволяет передавать через компьютерные сети письма, содержащие текст или файлы в двоичном коде (графические, звуковые, программы).

Почтовая служба основана на двух прикладных протоколах: *SMTP* и *POP3*. По *SMTP* происходит отправка корреспонденции с компьютера на сервер, а по *POP3* — прием поступивших сообщений.

Обеспечением *e-mail* занимаются специальные почтовые серверы. Почтовые серверы получают сообщения от клиентов и пересылают их по цепочке к почтовым серверам адресатов, где эти сообщения накапливаются. При установлении соединения между адресатом и его почтовым сервером происходит автоматическая передача поступивших сообщений на компьютер адресата.

Существует большое разнообразие клиентских почтовых программ. Например, *Microsoft Outlook Express*, входящая в состав операционной системы *Windows 98*; *The Bat!*; *Eudora Pro* и др. Эти программы выполняют следующие функции: подготовку текста; чтение, сохранение и удаление корреспонденции; ввод адреса; комментирование и пересылку корреспонденции; импорт (прием и преобразование в нужный формат) других файлов.

В *Internet* также существует множество служб бесплатной электронной почты. Например: Hotmail (<http://www.hotmail.com>); AltaVista (<http://altavista.digital.com>); Usa.net (<http://www.usa.net>); Mail.ru (<http://www.mail.ru>) и др.

Отличием этих служб от почты получаемой через провайдера с помощью почтовой программы является то, что работа с бесплатным почтовым ящиком происходит с помощью браузера. Универсальными качествами такой почты являются ее доступность из любой точки, с любого компьютера имеющего выход в *Internet* на котором есть браузер и достаточно большой уровень анонимности.

Адрес электронной почты состоит из **имя_пользователя@сервер.домен**

Основные операции при работе с электронной почтой

Регистрация электронного ящика

- 1) В строке адрес введите адрес почтового сервера www.mail.ru
- 2) На открывшейся странице выберите пункт *Регистрация*;
- 3) Прочтите соглашение об использовании и нажмите кнопку «Я принимаю условия».
- 4) На появившейся странице *Регистрация* заполните обязательные поля (отмеченные звездочкой) и нажмите кнопку *Дальше*;
- 5) Появится страница почтовой службы, работать в которой можно с помощью меню.

Подключение к почтовой службе

- 1) В строке адрес введите адрес почтового сервера
- 2) Заполните поля *Имя* и *Пароль* и нажмите кнопку *Проверить почту*.

Просмотр почты

- 1) Выберите пункт *Входящие*.
- 2) Откройте нужное письмо двойным щелчком
- 3) Просмотреть всю почту можно используя кнопки *Предыдущее* и *Последующее*.

Отправка почты

- 1) Выберите пункт *Написать письмо*.
- 2) Заполните поля *Кому* и *Тема* в заголовке письма.
- 3) Вставьте текст письма.
- 4) Нажмите кнопку *Отправить*.

Замечание. Прочитав письмо, вы можете сразу ответить на него. Для этого выберите пункт *Ответить на письмо*, при этом поля заголовка заполнятся автоматически. Затем введите текст письма и щелкните по кнопке *Отправить*.

Запись полученного письма на диск

- 1) Сделайте щелчок мышью в окне с текстом письма;
- 2) Выберите в управляющем меню *Файл*, команду *Сохранить как файл*;
- 3) Заполните необходимые поля появившегося диалогового окна;
- 4) Нажмите кнопку *Сохранить*.

Вывод текста письма на принтер

- 1) Сделайте щелчок мышью в окне с текстом письма;
- 2) Выберите в управляющем меню *Файл*, команду *Печать*.

ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ:

1 задание. Определите цифровой IP-адрес своего компьютера

1.1. Создайте в текстовом процессоре *MSWord* документ:

- a) Введите в него заголовок «Отчет по лабораторной работе №2».
- b) Задайте параметры страницы:

- все поля по 2 см;
- номер страницы вверху справа;
- верхний колонтитул (размер шрифта 10): первая строка *Ваша фамилия, № группы, ПК_№(№ – номер вашего ПК)* вторая строка автотекст *Полное имя файла и Дата создания* (выравнивание по левому краю).

c) Сохраните документ в папке *лаб_2* (необходимо создать), в Вашем каталоге под именем *Отчет2*.

1.2. Откройте в ОС *Windows 98* окно *Сеанс MS-DOS*: *Пуск* → *Программы* → *Сеанс MS-DOS*

или в ОС *Windows XP* окно *Командная строка*: *Пуск* → *Программы* → *Стандартные* → *Командная строка*

1.3. В открывшемся окне, после приглашения ОС *MS-DOS* введите команду **ipconfig** и нажмите клавишу *ENTER*.

1.4. Сделайте *Screenshot* окна и вставьте его в Ваш документ *Отчет2*.

1.5. Закройте окно *Сеанс MS-DOS*.

2 задание. Работа с папкой Избранное

2.1. Запустите программу *Internet Explorer*.

2.2. На панели *Адрес* введите: <http://alexovo.narod.ru/indexgv.htm>

2.3. Просмотрите загруженную страницу.

2.4. Из контекстного меню рабочей области программы выберите в команду *Добавить в Избранное*.

2.5. В поле *Имя* введите: *Экспериментальная страница*.

2.6. Щелкните на кнопке *ОК*.

2.7. Щелкните на кнопке *Домой* на панели инструментов.

2.8. Выполните команду *Избранное* → *Экспериментальная страница*.

2.9. Убедитесь, что в папке *Избранное* действительно была сохранена информация о загружаемой странице.

2.10. Выполните команду *Избранное* → *Упорядочить избранное*. Щелкните на кнопке *Создать папку*. Дайте новой папке имя *Материалы*.

2.11. Выберите пункт *Экспериментальная страница*. Щелкните на кнопке *Переместить*.

2.12. В диалоговом окне *Обзор папок* выберите папку *Материалы*, после чего щелкните на кнопке *ОК*.

2.13. Закройте диалоговое окно *Упорядочить избранное* и программу *Internet Explorer*. Разрывать соединение с *Интернетом* не следует!

2.14. Выполните команду *Пуск* → *Избранное* → *Материалы* → *Экспериментальная страница*.

2.15. Ознакомьтесь с тем, какая страница при этом загружается.

2.16. Продемонстрируйте результаты преподавателю.

2.17. Уничтожьте папку *Материалы* и все ее содержимое.

3 задание. Работа с FTP-архивом в Интернет

3.1. На панели *Адрес* введите: <ftp://ftp.microsoft.com/>

3.2. Внимательно рассмотрите способ представления каталога архива *FTP* в программе *Internet Explorer*.

3.3. Сделайте *Screenshot* окна и вставьте его в Ваш документ *Отчет2*. Обратите внимание на то, как выглядит значок в строке адреса.

3.4. Двойными щелчками на значках папок откройте папку */Products/Windows/Windows95/CDRomExtras/FunStuff/*.

3.5. В контекстном меню значка **clouds.exe** выберите пункт *Копировать в папку*.

3.6. В появившемся диалоговом окне, выберите папку *лаб_2* из своего каталога для сохранения файла.

3.7. В диалоговом окне загрузки файла установите флажок *Закрывать диалоговое окно после завершения загрузки*.

3.8. Следите за ходом загрузки файла по этому диалоговому окну.

3.9. Убедитесь, что сохраненный файл находится в папке *лаб_2* Вашего каталога, открыв ее, при помощи программы *Проводник*.

4 задание. Настройка Web-браузера Internet Explorer

4.1. Установите *Домашнюю страницу*, с которой следует начинать обзор *about:blank* (*С пустой*)

а) Откройте окно обозревателя *Internet Explorer*.

б) Выполните команду *Сервис* → *Свойства обозревателя*, воспользовавшись управляющим меню.

в) В диалоговом окне *Свойства обозревателя* на вкладке *Общие* в поле *Домашняя страница* щелкните по командной кнопке *С пустой*.

г) В поле *Временные файлы Интернета* щелкните по командной кнопке *Удалить файлы*.

е) Щелкните на кнопке *ОК*.

4.2. Настройка отображения объектов

а) Выполните команду *Сервис* → *Свойства обозревателя*.

б) Откройте вкладку *Дополнительно*.

в) Сбросьте флажки *Воспроизводить анимацию*, *Воспроизводить звуки*, *Воспроизводить видео*, *Отображать рисунки*.

г) Щелкните на кнопке *ОК*.

е) На панели *Адрес* введите: <http://alexovo.narod.ru/indexgv.htm>

ф) Щелкните на одной из пустых рамок для рисунков правой кнопкой мыши, и выберите в контекстном меню команду *Показать рисунок*.

4.3. Смена кодировки вывода Web-страницы

а) Используя управляющее меню обозревателя, смените кодировку вывода страницы с *Win-1251* на *KOI-8* и наоборот командой: *Вид* → *Кодировка* → ... (выбрать необходимую).

4.4. Знакомство с настройками свойств обозревателя для фильтрации негативной информации

- a) Выполните команду *Сервис* → *Свойства обозревателя*, воспользовавшись управляющим меню.
- b) В диалоговом окне *Свойства обозревателя* на вкладке *Безопасность* щелкните по командной кнопке *Другой*.
- c) В диалоговом окне *Параметры безопасности* посмотрите, какие существуют параметры (ничего не изменять, только посмотреть).
- d) Щелкните на кнопке *Отмена*, для закрытия окна *Параметры безопасности*.
- e) В диалоговом окне *Свойства обозревателя* на вкладке *Содержания* посмотрите, какие есть элементы управления для *ограничения доступа к информации, получаемой из Интернет*.
- f) Щелкните на кнопке *Отмена*, для закрытия окна *Свойства обозревателя*.

5 задание. Работа с электронной почтой

- 5.1. Загрузите страницу бесплатного почтового сервера *mail.ru* (www.mail.ru);
- 5.2. Пройдите регистрацию и получить электронный почтовый ящик на сервере *mail.ru*;
- 5.3. Запомните (запишите) электронный адрес и пароль;
- 5.4. Выбрать пункт *Помощь* и ознакомиться с назначением пунктов *Папки, Адреса, Настройки*;
- 5.5. Прочтите письмо службы технической поддержки в папке *Входящие*;
- 5.6. Отправьте письма одноклассникам, узнав их адреса;
- 5.7. Выйдите из почтовой службы (Отключитесь);
- 5.8. Подключитесь к почтовой службе *mail.ru*;
- 5.9. Просмотрите почту и сохраните одно из полученных писем в папке *лаб_2* Вашего каталога;
- 5.10. Ответите на полученные письма;
- 5.11. В адресную книгу внесите адреса (не менее 2) одноклассников;
- 5.12. Напишите поздравительное письмо однокласснику, воспользовавшись вкладкой *Расширенный формат*, для создания форматированного письма с разным начертанием и цветом шрифта, вставив подходящие смайлики и жесты, прикрепив к своему письму заранее созданный графический файл. Для вставки адреса воспользуйтесь адресной книгой.
- 5.13. Найдите и прочитайте письмо с вложением. Сохранить его в папке *лаб_2* Вашего каталога.
- 5.14. Сделайте распечатку одного из полученных писем.
- 5.15. Сделайте *Screenshot* окна с *Адресной книгой* и вставьте его в Ваш документ *Отчет2*.
- 5.16. Сделайте *Screenshot* окна с отображением *списка писем* в папке *Входящие*, и вставьте его в Ваш документ *Отчет2*.
- 5.17. Отправьте письмо преподавателю, указав свою фамилию и номер группы в тексте письма и приложив к нему свой отчет о работе (*Отчет2*).

6 задание. Знакомство с поисковой системой Yandex

- 6.1. На панели *Адрес* программы *Internet Explorer* введите адрес поисковой системы: <http://www.yandex.ru/>
- 6.2. Внимательно рассмотрите загруженную страницу, найдите поле для ввода ключевых слов и кнопку запуска поиска, перечень каталогов.
- 6.3. Найдите ссылку *Помощь* и ознакомьтесь с разделом *Как искать в Яндексе*.
- 6.4. Необходимую информацию сохраните в папке *лаб_2* Вашего каталога.
- 6.5. На панели *Адрес* программы *Internet Explorer* введите адрес <http://www.allbest.ru/union/> для просмотра сайта, на котором находится список *образовательных ресурсов*. Просмотрите наиболее интересные для вас ссылки.

7 задание. Поиск информации по ключевым словам (выполняется по вариантам)

- 7.1. В поле для ввода ключевых слов введите ключевые слова по своему варианту.
- 7.2. Щелкните на кнопке *Найти*.
- 7.3. Просмотрите результаты поиска.
- 7.4. Просмотрите всю первую группу ссылок на найденные страницы. Необходимую информацию по предложенной теме сохраните в папке *лаб_2* Вашего каталога:
 - a) Адрес страниц (используя буфер обмена и ссылку).
 - b) Графические изображения (не менее 3).

- с) Текст в формате типа:
 - Текстовый файл (*.txt);
 - Веб-страница, полностью (*.htm, *.html);
 - Веб-страница, только HTML (*.htm, *.html).
- д) Фрагмент текста с *Web-страницы*.
- е) Видеоизображения, анимацию, gif-файлы, звуковые файлы (если такая информация будет).

8 задание. Поиск информации в каталогах

8.1. Используя систему вложенных каталогов, выберите каталог (раздел, ссылку), соответствующий вашей теме.

8.2. Найдите в нем документы (2-3) соответствующие вашей теме, и сохраните их в папке *лаб_2* Вашего каталога. Просмотрите скаченные документы. Ненужные удалите.

9 задание. Работа с коллекцией рефератов

9.1. Загрузите коллекцию рефератов <http://www.referats.ru/>

9.2. Найдите реферат по теме варианта.

9.3. Скачайте файл этого реферата в папку *лаб_2* Вашего каталога.

9.4. Просмотрите его содержание после разархивации.

10 задание. Продемонстрируйте преподавателю результаты работы: папку *лаб_2* Вашего каталога с файлами *Отчет2.doc*, из заданий 3, 5-9

КОНТРОЛЬНЫЕ ВОПРОСЫ:

1. Что такое IP-адрес? Какие две формы записи имеет IP-адрес?
2. Что такое протокол? Виды и назначение протоколов?
3. Что такое эталонная модель *OSI*? Перечислите уровни и их функции.
4. Что называется браузером, *Web-страницей*, *Web-сервером*, *HTML*? Приведите примеры браузеров?
5. Какие настройки можно сделать в обозревателе *Internet Explorer* и для чего?
6. Как настроить обозреватель *Internet Explorer*, чтоб *Web-страницы* загружались быстрее?
7. Какая информация может находиться на *Web-странице*, в какой кодировке она может быть записана?
8. Что называется гипертекстовой ссылкой, как она выглядит на странице?
9. Как перейти на *Web-страницу* с определенным именем?
10. Как вернуться на предыдущую страницу?
11. Как оставить закладку в папке *Избранное*? Назначение папки *Избранное*?
12. Как записать адрес *Web-страницы* на диск А:?
13. Как воспользоваться сделанными закладками?
14. Как записать все содержимое страницы на диск?
15. Как записать часть содержимого страницы на диск?
16. В каком формате можно записать страницу?
17. Как записать графический объект?
18. В каком виде представлены файлы с рефератами?
19. Как записать файл с рефератом на диск А:?
20. Как подключиться к почтовой службе?
21. Как получить электронный ящик на почтовом сервере?
22. Для чего предназначен пункт *Папки*?
23. Для чего предназначен пункт *Адреса*? *Настройки*?
24. Как просмотреть почту?
25. Как отправить письмо? Ответить на письмо?
26. Как написать отформатированное письмо?
27. Как записать полученное письмо на диск? Как вывести текст письма на принтер?
28. Какой вид имеет электронный адрес?

ВАРИАНТЫ К ЗАДАНИЯМ 7-9

№	Тема	№	Тема	№	Тема
---	------	---	------	---	------

1.	Аквариумные рыбки
4.	Акробатика
7.	Алмазный фонд
10.	Бальные танцы
13.	Большие птицы
16.	Большой теннис
19.	Великие храмы России
22.	Виды легкой атлетики
25.	Владимир Высоцкий
28.	Гимнастика
31.	Города-герои России
34.	Грызуны
37.	Декоративные цветы
40.	Доисторические животные
43.	Долгожители среди животных
46.	Долгожители среди птиц
49.	Домашние птицы
52.	Екатериновский дворец
55.	Животные и птицы Антарктиды
58.	Животные, занесенные в Красную книгу
61.	Животный мир Австралии
64.	Животный мир Азии
67.	Животный мир

2.	История самолетостроения
5.	История подводного флота
8.	Легенды звездного неба
11.	Ливерпульская четверка
14.	Лиственные деревья
17.	Лошади
20.	Лувр
23.	Любимый актер
26.	Любимый певец
29.	Мир акул
32.	Мир китов
35.	Мир кораллов
38.	Морские животные
41.	Морские рыбы
44.	Награды Российской империи
47.	Награды Советского периода
50.	Обезьяны
53.	Овощи
56.	Оптические явления в кристаллах и камнях
59.	Российские художники передвижники
62.	Павловский дворец
65.	Памятные места Уссурийска
68.	Пауки

3.	Растительный мир Африки
6.	Растительный мир Европы
9.	Рептилии
12.	Российские космонавты
15.	Полевые цветы
18.	Оружие самообороны
21.	Самые большие животные
24.	Самые высокие точки мира
27.	Самые маленькие животные
30.	Сельскохозяйственные животные
33.	Семь чудес света
36.	Символика России и Российской империи
39.	Собаки
42.	Спортивные танцы
45.	Стрелковое оружие
48.	Устройство ПК
51.	Уфология
54.	Фауна Приморского края
57.	Физико-математический факультет
60.	Фигурное катание
63.	Флора Приморского края
66.	Фрукты
69.	Хвойные деревья

	Америки				
70.	Животный мир Африки	71.	Петергоф и его фонтаны	72.	Холодное оружие
73.	Животный мир Европы	74.	Подводный растительный мир	75.	Чарли Чаплин (Спенсер)
76.	Животный мир Северного полуса	77.	Российские Нобелевские лауреаты	78.	Достопримечательности Владивостока
79.	Змеи Приморского края	80.	Прадо	81.	Эрмитаж
82.	Знаки зодиака	83.	Различные единоборства	84.	Ягоды
85.	Знаменитые вулканы	86.	Разнообразие кактусов	87.	Ядовитые змеи
88.	Игровые виды спорта	89.	Разнообразный мир попугаев	90.	Кошки
91.	История воздухоплавания	92.	Растительный мир Америки	93.	Растения, занесенные в Красную книгу
94.	История кораблестроения	95.	Растительный мир Австралии	96.	Мировые курорты
97.	История машиностроения	98.	Растительный мир Азии	99.	Экзотические деревья

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 40
Инструменты управления сервером

Цель. Научиться включать на сервере программу *Удаленный рабочий стол для администрирования*; включать пользователей в соответствующую группу, чтобы разрешить им удаленно администрировать сервер; подключаться к серверу с помощью программы *Удаленный рабочий стол для администрирования*.

Оборудование. Компьютер с установленной ОС Windows Server 2003 (сервер должен иметь имя Server01 и быть контроллером домена contoso.com); служебная программа *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration), установленная на Server01, с включенными функциями *Дистанционное управление рабочим столом* (Remote Desktop); сконфигурированная и работающая по протоколу TCP/IP сеть, к которой могут подключаться консоль и удаленно администрируемые компьютеры.

Теоретическое обоснование.

В семействе Windows 2000 Server был впервые реализован тесно интегрированный набор программных средств и технологий, позволяющих выполнять удаленное администрирование и совместно использовать приложения с помощью *Служб терминалов* (Terminal Services). Эволюция продолжилась: отныне службы терминалов — неотъемлемый компонент семейства Windows Server 2003, а инструмент *Дистанционное управление рабочим столом* (Remote Desktop) усовершенствован и позиционируется как стандартная функция. Так что теперь достаточно одного щелчка мыши, и компьютер с Windows Server 2003 будет параллельно обрабатывать до двух подключений удаленного администрирования. Добавив компонент *Сервер терминалов* (Terminal Server) и настроив соответствующую лицензию, администратор добьется еще большего эффекта: множество пользователей смогут запускать приложения на сервере. На этом занятии вы научитесь работать со служебной программой *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

Включение и конфигурирование программы *Удаленный рабочий стол для администрирования*.

Службы терминалов позволяют совместно использовать приложения с помощью таких инструментов, как *Дистанционное управление рабочим столом* (Remote Desktop), *Удаленный помощник* (Remote Assistance) и *Сервер терминалов* (Terminal Server). По умолчанию служба устанавливается вместе с Windows Server 2003 и настраивается в программе *Дистанционное управление рабочим столом* для работы в режиме удаленного администрирования: допускает только два параллельных удаленных подключения и не содержит компоненты для совместного использования приложений из состава *Сервера терминалов*. Следовательно, *Дистанционное управление рабочим столом* создает очень небольшую дополнительную нагрузку на систему, причем не требует дополнительного лицензирования.

Примечание Поскольку *Службы терминалов* и *Дистанционное управление рабочим столом* являются стандартными компонентами Windows Server 2003, каждый сервер способен поддерживать удаленные подключения к своей консоли. Термин «сервер терминалов», таким образом, теперь по праву можно применить к любому компьютеру под управлением Windows Server 2003, обеспечивающему совместное использование приложений несколькими клиентами за счет добавления компонента *Службы терминалов*.

Другие компоненты — *Сервер терминалов* и службу *Лицензирование сервера терминалов* (Terminal Server Licensing) — нужно добавлять с помощью функции *Установка и удаление программ* (AddOrRemovePrograms). Тем не менее, все средства администрирования для настройки и поддержки клиентских подключений и управления сервером терминалов устанавливаются по умолчанию на все компьютеры с Windows Server 2003. Эти средства и их функции описаны в таблице 1.

Таблица 1. Стандартные компоненты Сервер терминалов и Подключение к удаленному рабочему столу

Установленное ПО	Назначение
<i>Настройка служб терминалов</i> (Terminal Services Configuration)	Настройка свойств сервера терминалов, в том числе параметров сеанса, сети, клиентского рабочего стола и удаленного управления клиентом

<i>Диспетчер служб терминалов</i> (Terminal Services Manager)	Отправка сообщений клиентам, подключенным к серверу терминалов, отключение или завершение сеансов, а также инициирование удаленного управления или маскировки сеансов
<i>Подключение к удаленному рабочему столу</i> (Установочные файлы клиента RemoteDesktopConnection)	Установка клиентского приложения <i>Дистанционное управление рабочим столом</i> (Remote Desktop) для Windows Server 2003 или Windows XP. 32_разрядное клиентское ПО <i>Дистанционное управление рабочим столом</i> устанавливается в папку %Systemroot%\System32\Clients\Tsclient\Win32 на сервере терминалов
<i>Лицензирование служб терминалов</i> (Terminal Services Licensing)	Настройка лицензий для клиентских подключений к серверу терминалов. Это средство не подходит для сред, где используется только <i>Удаленный рабочий стол для администрирования</i>

Чтобы разрешить подключения *Дистанционное управление рабочим столом* (Remote Desktop) на компьютере под управлением Windows Server 2003, в *Панели управления* выберите Система (System Properties). На вкладке Удаленное использование (Remote) выберите **Разрешить удаленный доступ к этому компьютеру (Allow Users To Connect Remotely To This Computer)**.

Примечание Если сервер терминалов является контроллером домена, необходимо также настроить групповую политику контроллера, чтобы разрешить группе *Пользователи удаленного рабочего стола* (Remote Desktop Users) подключение посредством служб терминалов. На серверах, не являющихся контроллерами домена, подключение через службы терминалов пользователям из этой группы разрешено по умолчанию.

Подключение к удаленному рабочему столу.

Подключение к удаленному рабочему столу (Remote Desktop Connection) — это клиентское приложение, используемое для подключения к серверу в контексте режима *Дистанционное управление рабочим столом* (Remote Desktop) или *Сервер терминалов* (Terminal Server). Для клиента нет функциональных различий между этими двумя конфигурациями сервера.

На компьютерах с Windows XP и Windows Server 2003 программа *Подключение к удаленному рабочему столу* установлена по умолчанию, но глубоко запрятана: **Пуск (Start)\Все программы (All Programs)\Стандартные (Accessories)\Связь (Communications)\Подключение к удаленному рабочему столу (Remote Desktop Connection)**.

На других платформах программу *Подключение к удаленному рабочему столу* можно установить с компакт-диска Windows Server 2003 либо из установочной папки клиента (%Systemroot%\System32\Clients\Tsclient\Win32) на любом из компьютеров под управлением Windows Server 2003. Установочный пакет MSI можно распространять на системы Windows 2000 с помощью групповой политики или средствами SMS (Systems Management Server).

Совет Рекомендуется обновить предыдущие версии клиента *Служб терминалов*, установив последнюю версию *Подключение к удаленному рабочему столу*, чтобы обеспечить наиболее оптимальную, безопасную и стабильную среду, поскольку в этом случае будет доступен улучшенный пользовательский интерфейс, 128_битное шифрование и выбор альтернативных портов.

На рисунке 2 показан клиент программы *Дистанционное подключение к рабочему столу*, настроенный для подключения к серверу Server01 в домене contoso.com.

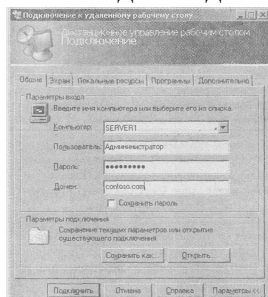


Рисунок 2. Клиент программы *Удаленное подключение к рабочему столу*
Настройка клиента удаленного подключения к рабочему столу.

Вы можете управлять множеством аспектов дистанционного подключения как со стороны клиента, так и со стороны сервера. В таблице 2 перечислены конфигурационные параметры и их назначение.

Таблица 2. Параметры программы Удаленное подключение к рабочему столу

Параметры	Назначение
Параметры клиента	
Общие (General)	Параметры выбора компьютера, к которому необходимо подключаться, настройка статических реквизитов для входа в систему, а также сохранение параметров для данного подключения
Экран (Display)	Задаёт размер окна клиента, глубину цвета, а также доступность панели подключений при работе в полноэкранном режиме
Локальные ресурсы (Local Resources)	Параметры передачи звуковых событий на локальный компьютер, помимо стандартных выходных сигналов мыши, клавиатуры и экрана. Также параметры на этой вкладке определяют, как удаленный компьютер интерпретирует комбинации клавиш Windows (например Alt+Tab), и доступны ли в сеансе удаленного доступа такие устройства, как локальные диски, принтеры и последовательные порты
Программы (Programs)	Задаёт путь и папки расположения для любых программ, которые необходимо запустить после установки соединения
Дополнительно (Experience)	Категории функций экрана можно включать или отключать в зависимости от пропускной способности канала связи между локальным и удаленными компьютерами. Предусмотрены параметры для отображения фона рабочего стола, содержимого окна при перетаскивании, визуальных эффектов при прорисовке меню и окон, тем рабочего стола; также вы можете активировать режим кэширования растровой графики, при котором после каждого интервала обновления передаются только изменения, а не весь экран целиком
Параметры сервера	
Параметры входа (Logon Settings)	Позволяет задать статические реквизиты для подключения вместо реквизитов, предоставляемых клиентом
Сеансы (Sessions)	Чтобы перекрыть настройки клиента, задайте здесь параметры завершения прерванного сеанса, ограничения длительности сеанса и времени его простоя, а также допустимость повторного подключения
Среда (Environment)	Перекрывает настройки из профиля пользователя для данного подключения в отношении запуска программы: здесь вы можете переопределить запускаемую при подключении программу. Заданный здесь путь и папка запуска приоритетнее настроек, сделанных программой <i>Подключение к удаленному рабочему столу</i>
Разрешения (Permissions)	Позволяет задавать дополнительные разрешения для данного подключения
Удаленное управление (Remote Control)	Указывает, можно ли удаленно управлять сеансом <i>Подключение к удаленному рабочему столу</i> , и если так, то должен ли пользователь выдавать разрешение на инициализацию сеанса удаленного управления. Дополнительные параметры позволяют ограничить сеанс удаленного управления только функцией просмотра либо разрешить полную интерактивность с сеансом клиента <i>Дистанционное управление рабочим столом</i>
Параметры клиента (Client Settings)	Позволяют перекрыть параметры из конфигурации клиента, изменить глубину цвета и отключить различные коммуникационные порты (порты ввода-вывода)
Сетевой адаптер (Network)	Указывает, какие сетевые платы на сервере будут принимать удаленные подключения для администрирования

Adapters)	
Общие (General)	Задаёт уровень шифрования и механизм проверки подлинности для подключений к этому серверу

Устранение неполадок при работе со службами терминалов.

При использовании программы *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration) создается подключение к консоли сервера. Есть несколько потенциальных причин неудачных подключений или сеансов с ошибками.

- **Сбои сети.** Ошибки в работе стандартной TCP/IP_сети могут вызывать сбои или разрывы подключений *Дистанционное подключение к рабочему столу* (Remote Desktop). Если не функционирует служба DNS, клиент не сможет найти сервер по имени. Если не функционирует маршрутизация либо неверно настроен порт *Служб терминалов* (Terminal Services) (по умолчанию это порт 3389) на клиенте или сервере, соединение установить не удастся.

- **Реквизиты входа.** Для успешного подключения к серверу средствами программы *Удаленный рабочий стол для администрирования* пользователи должны быть включены в группу *Администраторы* (Administrators) или *Пользователи удаленного рабочего стола* (Remote Desktop Users).

Если подключиться через *Удаленный рабочий стол для администрирования* не удастся из-за запрета доступа, проанализируйте членство в группах. В предыдущих версиях *Сервера терминалов* (Terminal Server) для подключения к серверу требовалось быть участником группы *Администраторы* (Administrators), хотя специальные разрешения можно было выдать вручную. Сервер терминалов поддерживает только два удаленных подключения.

- **Политика.** Только администраторам разрешено подключаться средствами программы *Дистанционное подключение к рабочему столу* (Remote Desktop) к контроллерам доменов. Чтобы разрешить подключаться остальным пользователям, нужно настроить политику безопасности на контроллере домена.

- **Слишком много параллельных подключений.** Если сеансы прерывались без выхода из системы, сервер может посчитать, что достигнут предел одновременно обрабатываемых подключений, даже если в данный момент к серверу не подключены два пользователя. Например, администратор может завершить сеанс без выхода из системы. Если еще два администратора попытаются подключиться к серверу, это удастся только одному из них.

Часть 1. Настройка удаленного подключения к рабочему столу

В этом задании вы активируете удаленное подключение к рабочему столу, измените число разрешенных одновременных подключений на сервере и настройте параметры завершения подключения.

1. Войдите на Server01 как *Администратор* (Administrator).
2. В Панели управления выберите **Система (System Properties)**.
3. На вкладке **Remote (Удалённое использование)** включите **Remote Desktop (Включить удалённый рабочий стол)**. Закройте окно **Система (System Properties)**.
4. Откройте консоль *Настройка служб терминалов* (Terminal Services Configuration) из группы программ *Администрирование* (Administrative Tools).
5. В консоли tssc (TerminalServicesConfiguration\Connections) на правой панели щелкните правой кнопкой подключение **RDP_tcp** и выберите **Свойства (Properties)**.
6. На вкладке **Сетевой адаптер (Network Adapter)** установите значение параметра **Максимальное число подключений (Maximum Connections)** равным 1.
7. На вкладке **Сеансы (Sessions)** установите оба флажка **Заменить параметры пользователя (Override User Settings)** и измените настройки следующим образом: все прерванные любыми способами (или по любой причине) сеансы пользователей закрываются через 15 минут, активный сеанс не ограничивается по времени, сеансы завершаются после 15 минут бездействия.

- **Завершение отключенного сеанса (End a disconnected session):** 15 минут,
- **Ограничение активного сеанса (Active session limit):** никогда (never),
- **Ограничение активного сеанса (Active session limit):** 15 минут.
- **При превышении ограничений или разрыве подключения (When session limit is reached or connection is broken):** Отключить сеанс (Disconnect from session).

Такая конфигурация обеспечивает следующее: только один пользователь одновременно подключен к серверу терминалов, любой прерванный сеанс закроется через 15 минут и неактивный сеанс прервется через 15 минут. Эти параметры позволяют избежать ситуации, когда прерванный или бездействующий сеанс мешает подключаться средствами программы *Удаленный рабочий стол для администрирования* (RemoteDesktopforAdministration).

Часть 2. Подключение к серверу с помощью клиента удаленного подключения к рабочему столу

1. На другой виртуальной машине в группе Стандартные\Связь (Accessories\Communications) щелкните **Подключение к удаленному рабочему столу (Remote Desktop Connection)**, подключитесь к Server01 и войдите в его систему.

2. На сервере Server01 откройте консоль tscc.msc: **Администрирование (Administrative tools)\Настройка служб терминалов (TerminalServicesConfiguration)**. В открывшейся консоли выберите **Подключения (Connections)**. Вы должны увидеть сведения о сеансе удаленного подключения к Server01.

3. Не выполняйте никаких действий в этом сеансе 15 минут либо закройте клиент программы *Удаленное подключение к рабочему столу* (Remote Desktop), не завершив сеанс *Сервера терминалов* (Terminal Server) явно: сеанс должен будет завершиться автоматически через 15 минут.

В данный момент вы подключены к Server01 удаленно и можете выполнять на нем любые задачи, допустимые в интерактивном режиме на консоли.

Контрольные вопросы.

1. Сколько одновременных подключений разрешено к серверу терминалов, работающему в режиме удаленного администрирования? Почему?

2. Как оптимальным образом предоставить администраторам возможность удаленного управления сервером через службы терминалов?

а. Не выполнять никаких действий; они уже имеют доступ, поскольку являются администраторами.

б. Удалить группу *Администраторы* (Administrators) из списка разрешений в подключении к серверу терминалов и поместить их административную учетную запись в группу *Удаленный рабочий стол для администрирования* (Remote Desktop for Administration).

в. Создать отдельную пользовательскую учетную запись с более низким уровнем авторизации для повседневного использования группой *Администраторы* и поместить ее в группу *Удаленный рабочий стол для администрирования*.

3. Какое программное средство используется на сервере для включения удаленного подключения к рабочему столу?

а. *Диспетчер служб терминалов* (Terminal Services Manager).

б. *Настройка служб терминалов* (Terminal Services Configuration).

в. *Система* (System Properties) из Панели управления.

г. *Лицензирование служб терминалов* (Terminal Services Licensing).

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова

Практическое занятие 41

Изучение средств анализа и управления сетями (утилиты аудита IP сети)

Цель работы: изучить основные сетевые команды.

Оснащение: МУ к ПЗ

Теоретические предпосылки

В Windows 2000 реализована общая консоль управления разработана для запуска всех программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие законченные модули называются оснастками (snap-in). Оснастки представляют собой управляющие компоненты, которые объединены в среде MMC. Консоль MMC включает в себя интерфейсы прикладного программирования (API), оболочку пользовательского интерфейса (консоли) и набор инструкций. Консоль управления имеет ряд преимуществ, которые заключаются в упрощении интерфейса, предоставлении больших возможностей по настройке разработанных решений для определенных административных проблем и в обеспечении различных уровней функциональности.

Преимущества MMC:

–*возможность индивидуальной настройки и передача полномочий.* MMC предоставляет возможность полностью индивидуальной настройки, так что администраторы могут создавать такие консоли управления, которые будут включать только необходимые им инструменты. Такая настройка позволяет ориентировать администрирование на выполнение конкретных задач, причем администратор может выделить только необходимые объекты и элементы. Настройка консоли также позволяет администраторам передавать определенную часть полномочий менее опытным сотрудникам. С помощью MMC можно создать консоль, которая будет содержать объекты, необходимые для выполнения только определенных функций;

–*интеграция и унификация.* MMC обеспечивает общую среду, в которой могут запускаться оснастки, и администраторы могут управлять различными сетевыми продуктами, используя единый интерфейс, что упрощает изучение работы с различными инструментами.

–*гибкость в выборе инструментов и продуктов.* В среде MMC можно использовать различные инструменты и оснастки. Для использования в среде MMC оснастка должна поддерживать объектную модель компонентов (ComponentObjectModel, COM) или распределенную COM (DistributedComponentObjectModel, DCOM). Это позволяет выбирать наиболее оптимальный продукт среди оснасток, причем гарантируется его полная совместимость со средой MMC.

Консоль управления MMC имеет пользовательский интерфейс, позволяющий открывать множество документов (MultipleDocumentInterface, MDI). Интерфейс консоли MMC на рисунке 4.1.

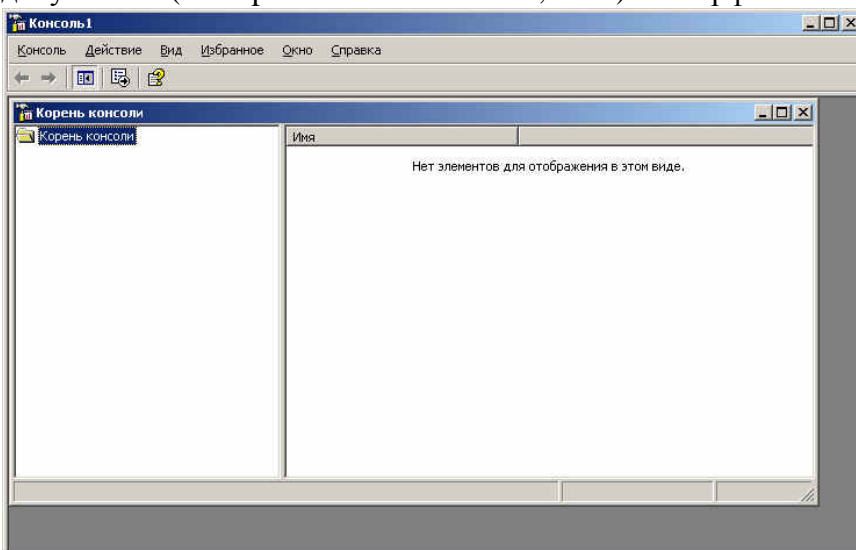


Рисунок 4.1

Родительское окно ММС имеет главное меню и панель инструментов. Главное меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе.

Дочерние окна ММС представляют собой различные средства просмотра автономного документа консоли. Каждое из этих дочерних окон содержит панель управления, панель структуры (scorepanel) и панель результатов, или сведений (resultpanel). Панель управления содержит меню и набор инструментов. Панель структуры отображает пространство имен инструментов в виде дерева, которое содержит все видимые узлы, являющиеся управляемым объектом, задачей или средством просмотра.

Панель результатов в дочернем окне отображает список элементов выбранного узла. Данный список может содержать папки, оснастки, элементы управления, web-страницы, панели задач и другие элементы.

Типы оснасток

В ММС поддерживаются два типа оснасток:

–изолированная оснастка (standalonesnap-in) обеспечивает выполнение своих функций даже при отсутствии других оснасток, например, **Управление компьютером** (Computermanagement);

–оснастка расширения (extensionsnap-in) может работать только после активизации родительской оснастки. Функция оснастки расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Оснастка расширения является подчиненным элементом узлов определенных типов, и при каждом запуске узлов данных типов консоль автоматически запускает все связанные с ней расширения. В качестве примера можно привести оснастку **Диспетчер устройств** (DeviceManager). Оснастки расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Создание новой консоли рассмотрим на следующем примере:

1. В меню **Пуск** выберите пункт **Выполнить**, введите **mmc** и нажмите кнопку **ОК**. Откроется окно **Консоль 1** с пустой консолью (или административным инструментом).
2. В меню **Консоль** (Console) выберите пункт **Добавить/удалить оснастку** (Add/RemoveSnap-in), после чего откроется окно **Добавить/Удалить оснастку**. В этом окне перечисляются изолированные оснастки и оснастки расширения, которые будут добавлены в консоль (или уже включены в нее). Оснастки можно добавлять к корню консоли управления или к уже имеющимся изолированным оснасткам (другим узлам дерева); это указывается в списке **Оснастки** (Snap-inaddedto). В нашем случае оставим значение по умолчанию — **Корень консоли** (ConsoleRoot).
3. Нажмите кнопку **Добавить** (Add). На экране появится окно **Добавить изолированную оснастку** (AddStandaloneSnap-in) со списком изолированных оснасток, имеющихся в системе.
5. Выполните двойной щелчок на пункте **Управление компьютером** (предварительно найдите эту оснастку в списке). Появится окно с конфигурационными опциями для данной оснастки.
6. Оставьте переключатель в положении **локальным компьютером** (LocalComputer). Затем нажмите кнопку **Готово** (Finish).
7. В окне оснасток выберите пункт **Сертификаты** и нажмите кнопку **Добавить**.
8. В следующем окне выберите соответствующий переключатель — **Эта оснастка всегда будет управлять сертификатами для: моей учетной записи пользователя** (Myuseraccount).
9. Нажмите кнопки **Готово** и **Заккрыть**.
10. В окне **Добавить/Удалить оснастку** (где отображен список подключаемых оснасток) перейдите на вкладку **Расширения** (Extensions). На этой вкладке приведен список оснасток расширения, которые поставляются вместе с выбранными изолированными оснастками. Если вы не собираетесь подключать все оснастки расширения, сбросьте флажок **Добавить все расширения** (AddAllExtensions) (который ставится по умолчанию) и снимите флажки с лишних оснасток. По окончании процедуры нажмите кнопку **ОК**.
11. Закройте окно добавления оснасток, нажав кнопку **ОК**. Теперь окно консоли содержит две оснастки — **Управление компьютером** и **Сертификаты** (рисунок 4.2).

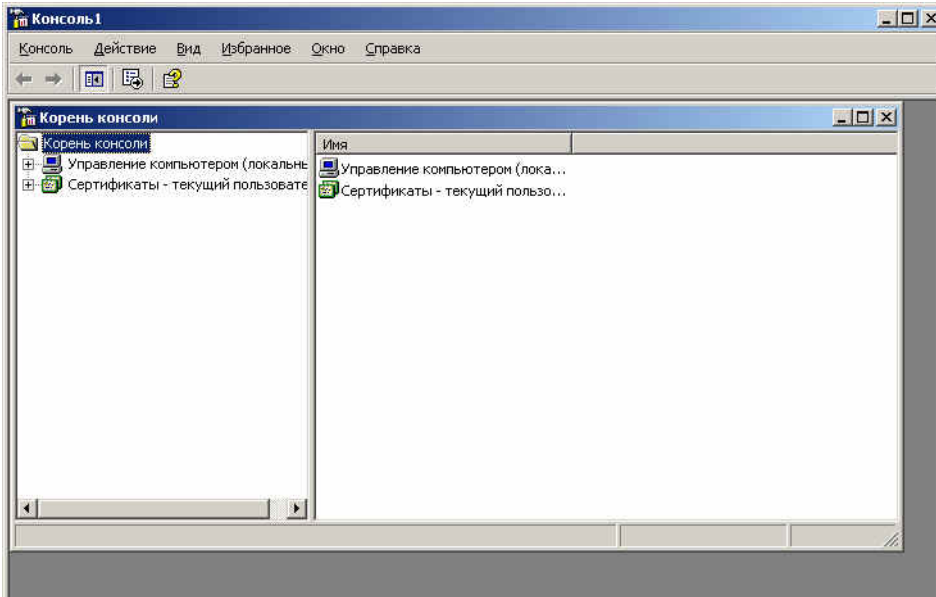


Рисунок 4.2

12. Для того чтобы сохранить созданный инструмент, в меню **Консоль** выберите пункт **Сохранить как** (SaveAs) и укажите имя файла и папку, в которой будет сохранен файл консоли.

Индивидуальная настройка окон оснасток

После добавления оснасток можно развернуть окна оснасток, чтобы облегчить работу с ними. Для этого выполните следующие действия:

1. В левом подокне (в окне структуры) только что созданной консоли щелкните правой кнопкой мыши на узле **Управление компьютером** и выберите в контекстном меню **Новое окно отсюда** (NewWindowfromHere). Будет открыто окно **Управление компьютером**, представляющее одноименную оснастку.
2. Аналогичные действия выполните для узла **Сертификаты**. В новом окне нажмите кнопку **Скрытие или отображение дерева консоли или избранного** (Show/HideConsoletree) на панели инструментов для того, чтобы скрыть панель структуры.
3. Закройте окно, содержащее корень консоли.
5. В меню **Окно** (Window) выберите команду **Сверху вниз** (TileHorizontally). Консоль будет выглядеть, как показано на рисунке 4.3.

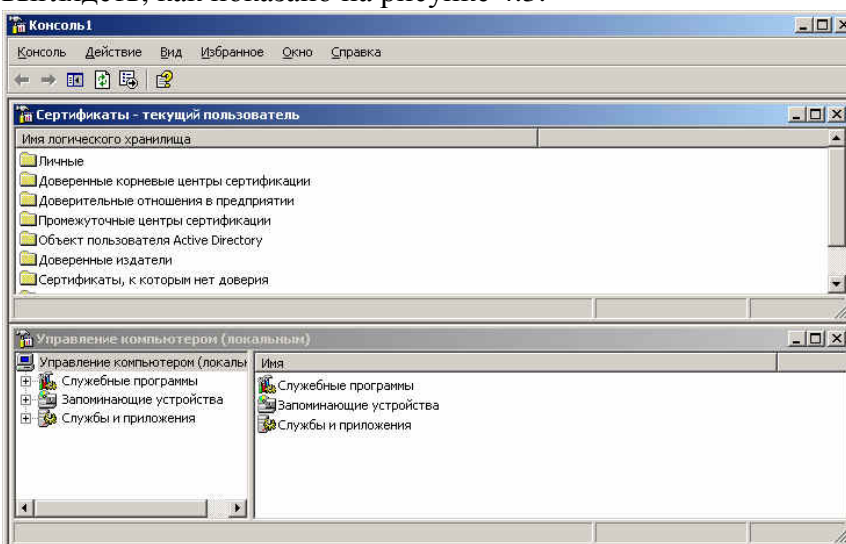


Рисунок 4.3

Создание панелей задач

Когда требуется создать файл консоли для другого пользователя, полезно предоставить пользователю упрощенный инструмент, позволяющий выполнять только несколько определенных задач. Таким инструментом является панель задач (taskpad). Панель задач является HTML-страницей,

на которой могут быть размещены ярлыки (или задачи (tasks)), запускающие команды меню и программы или открывающие ссылки на web-страницы.

Для создания панели задач выполните следующее:

1. В меню **Действие** (Action) или в контекстном меню любого узла в окне консоли выберите пункт **Новый вид панели задач** (NewTaskpadView).
2. Откроется окно **Мастера создания вида панели задач** (NewTaskpadViewWizard). Нажмите кнопку **Далее**.

В следующем окне мастера будет предложено выбрать стиль отображения и размер панели задач. Затем на панели задач можно указать использование только тех задач, которые связаны с текущим узлом или со всеми узлами дерева. В следующем окне потребуется ввести имя и описание создаваемой панели задач.

Если не требуется добавлять новые задачи на созданную панель, снимите в последнем окне мастера флажок **Запустить мастер создания новой задачи** (StartNewTaskWizard).

В противном случае по завершении работы **Мастера создания вида панели задач** запускается **Мастер создания задач** (NewTaskWizard). В ходе этой процедуры следует указать функцию задачи: запуск команды меню, программы или ссылка на web-страницу, ввести путь к исполняемому файлу и параметры запуска.

В остальных окнах мастера примите значения по умолчанию. Если требуется создать несколько задач на одной панели, установите в последнем окне мастера флажок **Запустить этот мастер снова** (Runthiswizardagain). Затем нажмите кнопку **Готово**.

На рисунке 4.4 показана созданная в результате панель задач. В данном окне консоли панель структуры отключена — аналогично тому, как это было сделано в предыдущем разделе. Для удаления лишних меню и панелей инструментов снимите соответствующие флажки в окне **Настройка вида** (CustomizeView) (опции оснастки в инструмент или удалять существующие, не сможет изменять свойства консоли, но будет иметь возможность изменять расположение окон. (Новый режим начнет работать при следующем запуске файла консоли). Если вы хотите еще ужесточить требования, то можете выбрать один из режимов ограничения – **Пользовательский режим** – **ограниченный допуск**.

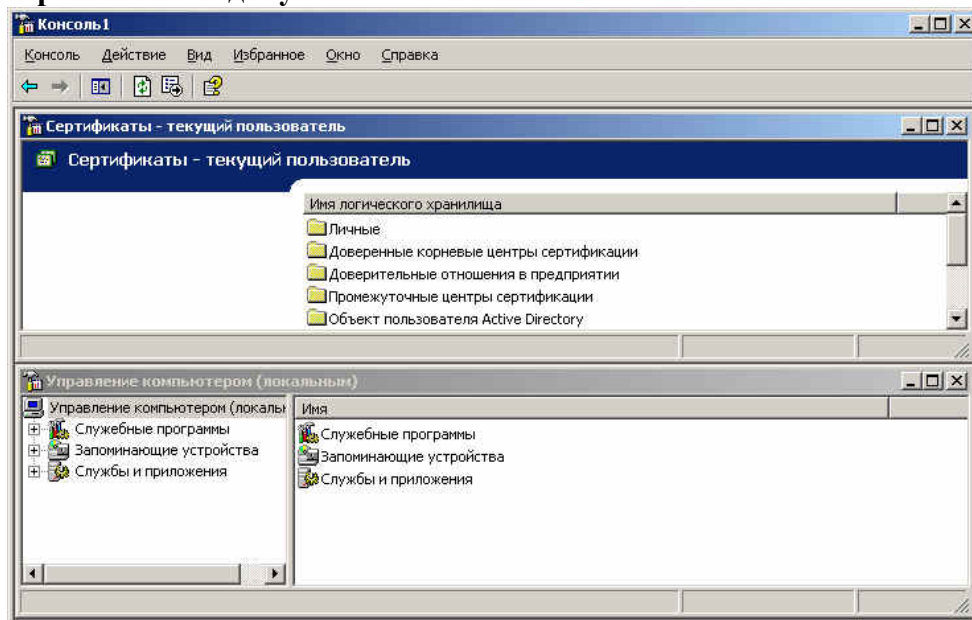


Рисунок 4.4

3. Сохраните файл.

Сохраненный файл консоли можно также открыть с помощью Проводника. Для этого выполните двойной щелчок на файле с расширением .msc. Файл консоли будет открыт в среде MMC.

Оснастки Windows 2000

В таблице 4.1 в алфавитном порядке перечислены основные оснастки, которые доступны в системе Windows 2000 Professional. Для оснасток, включенных в пользовательский интерфейс, указаны названия соответствующих пунктов меню, для остальных оснасток даны их собственные имена.

Оснастки, которые можно вызывать непосредственно из меню **Пуск** или из группы **Администрирование** на панели управления, т.е. оснастки, включенные в пользовательский интерфейс при инсталляции системы, - отмечены звездочкой (*)

Таблица 4.1

Оснастка	Назначение
Служба работы с факсами (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
Анализнастройкабезопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности
Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
Дефрагментация диска (Disk Defragmenter)	Служит для анализа и дефрагментации дисковых томов
Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
Локальные пользователи и группы (LocalUsersandGroups)	Служит для управления локальными учетными записями пользователей и групп
Общие папки Shared Folders)	Отображает совместно используемые папки, текущие сеансы и открытые файлы
Оповещение и журналы производительности (PerformanceLogsandAlerts)	Конфигурирует журналы данных о работе системы и службу оповещений
Папка (Folder)	Служит для добавления новой папки в дерево
Просмотр событий (Event Viewer)*	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Сведения о системе (System Information)	Отображает информацию о системе
Сертификаты (Certificates)	Служит для управления сертификатами
Системный монитор (Performance)*	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и других компонентов системы
Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
Служба компонентов (Component Services)*	Конфигурирует и управляет службами компонентов COM+
Службы (Services)*	Запускает, останавливает и конфигурирует службы (Services) Windows
Ссылканаресурс web (Link to Web Address)	Служит для подключения webстраниц (html, asp, stml)
Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т. д.
Управление компьютером (Computer Management)	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток расширения
Управление политикой безопасности IP (IPSecurityPolicyManagement)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами

Управление съемными носителями (RemovableStorageManagement)	Служит для управления съемными носителями информации
Управляющий элемент (WMI Control)	Служит для конфигурирования средств WindowsManagementInstrumentation и управления ими
Шаблоны безопасности (Security templates)	Обеспечивает возможность редактирования файлов-шаблонов безопасности
Элемент ActiveX (ActiveX Control)	Подключение к дереву консоли различных элементов управления ActiveX

Типовые задачи администрирования

Создание локальных учетных записей пользователей и групп

Создание учетных записей пользователей и групп занимает важное место в обеспечении безопасности Windows, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации, разрешить или запретить им выполнить в сети определенное действие, например, архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом — файлом или папкой. Оно определяет возможность данного пользователя получить доступ к объекту.

Оснастка Локальные пользователи и группы (LocalUsersandGroups)

Оснастка Локальные пользователи и группы - это инструмент MMC, с помощью которого выполняется управление локальными учетными записями пользователей и групп — как на локальном, так и на удаленном компьютерах. С ним можно работать на рабочих станциях и автономных серверах Windows 2000, как на изолированных, так и рядовых членах домена. На контроллерах домена Windows 2000 инструмент Локальные пользователи и группы недоступен, поскольку все управление учетными записями и группами в домене выполняется с помощью оснастки Пользователи и компьютеры ActiveDirectory(ActiveDirectoryUsersandComputers). Запускать оснастку Локальные пользователи и группы может любой пользователь. Выполнять администрирование учетных записей могут только администраторы и члены группы Опытные пользователи (PowerUsers).

Окно изолированной оснастки Локальные пользователи и группы выглядит аналогично показанному на рисунке 4.5.

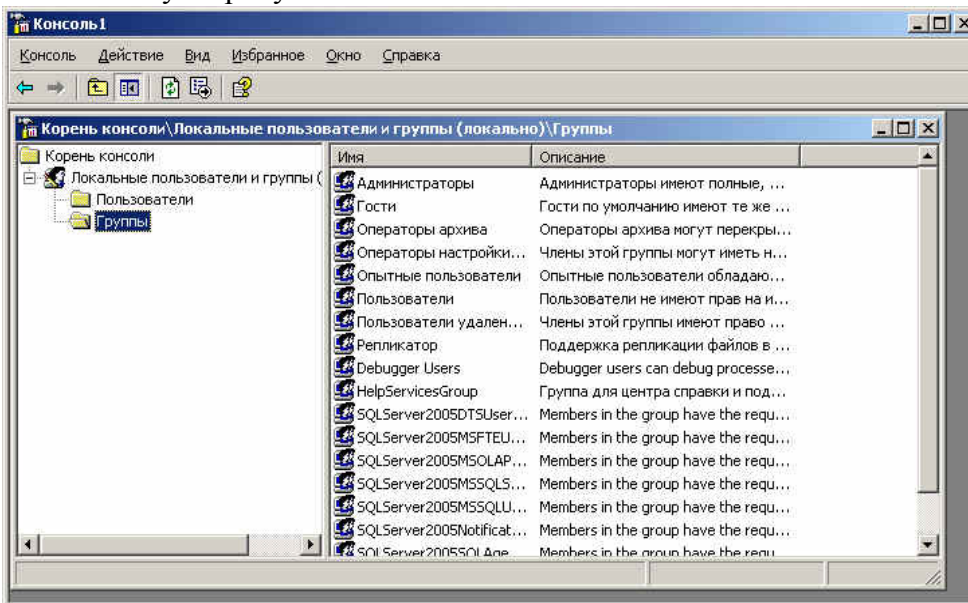


Рисунок 4.5

Папка Пользователи (Users)

Сразу после установки системы Windows (рабочей станции или сервера, являющегося членом домена) папка Пользователи содержит две встроенные учетные записи — Администратор

(Administrator) и Гость (Guest). Они создаются автоматически при установке Windows. Ниже даны описания свойств обеих встроенных учетных записей:

Администратор - эту учетную запись используют при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть уничтожена, заблокирована или удалена из группы Администраторы (Administrators), ее можно только переименовать.

Гость — эта учетная запись применяется в компьютере без использования специально созданной учетной записи. Учетная запись Гость не требует ввода пароля и по умолчанию заблокирована. Она является членом группы Гости (Guests). Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Папка Группы (Groups)

После установки системы Windows (рабочей станции или сервера, являющегося членом домена) папка Группы (Groups) содержит шесть встроенных групп. Они создаются автоматически при установке Windows. Ниже описаны свойства всех встроенных групп:

Администраторы (Administrators) - ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав.

Операторы архива (BackupOperators) - члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности.

Гости (Guests) — эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи Гость и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут за вершать работу системы.

Опытные пользователи (PowerUsers) - члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами Пользователи, Гости и Опытные пользователи. Члены группы Опытные пользователи не могут модифицировать членство в группах Администраторы и Операторы архива. Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий.

Репликатор (Replicator) — членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи.

Пользователи (Users) — члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер.

7. Изучите возможность создания сценариев входа в систему.

8. Ознакомьтесь с возможностями и настройкой подсистемы аудита, продемонстрируйте работу аудита на конкретном примере.

Список используемой литературы

Компьютерные сети: учебное пособие для студ. учреждений СПО/Н.В. Максимов, И.И. Попов – 5-е изд. перераб. и доп. – М.: ФОРУМ, 2012 – 464с.

Преподаватель

Н.А Мельникова