МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ

по дисциплине «Операционные системы»

Для студентов направления подготовки 09.03.02 Информационные системы и технологии, направленность (профиль) Информационные системы и технологии в бизнесе

Содержание

Лабораторная работа 1.
Исследование модели межсетевого взаимодействия

Цель работы: Ознакомиться с сетевыми утилитами, позволяющими тестировать разные уровни модели межсетевого взаимодействия

Теоретическая часть

Команда ping

Команда ping проверяет состояние соединения с другим компьютером или компьютерами, посылая эхо-пакеты протокола Internet Control Message Protocol (ICMP) и анализируя полученные ответы. Эта команда доступна только после установки поддержки протокола TCP/IP. Команда ping ждет до 1 секунды для каждого пакета и выводит число посланных и принятых пакетов. Каждый полученный пакет сравнивается с соответствующим посланным. По умолчанию четыре эхо-пакета содержат 64 байта данных (периодическая последовательность заглавных букв)

-t Выполнение команды до прерывания (Ctrl+C). Просмотр статистики и продолжение – (Ctrl+Break).

-a Разрешать IP-адреса в имена.

-n число отправляемых пакетов.

-l размер пакета.

По умолчанию 64 байта, максимум – 8192.

-f Установка флага, запрещающего фрагментацию пакета.

-i TTL. Задание времени жизни пакета (поле "Time To Live").

-v TOS. Задание типа службы (поле "Type Of Service").

-r число. Запись маршрута для указанного числа переходов, параметр задает число переходов в интервале от 1 до 9.

-s число. Задает число узлов на маршруте, где будет делаться отметка времени.

-j список узлов. Свободный выбор маршрута по списку узлов. Максимальное количество равно 9.

-k список узлов. Жесткий выбор маршрута по списку узлов. Максимальное количество равно 9.

-w интервал ожидания ответа в миллисекундах

Например, проверка связи с компьютером, имеющим IP-адрес 212.96.96.38:

ping 212.96.96.38

Вместо IP-адреса можно задать символьное доменное имя необходимого компьютера, например:

ping www.ncstu.ru

После ввода этой команды Windows сделает четыре попытки получения ответа от соответствующего компьютера. При этом на экран выводиться время, которое было необходимо для получения ответа на ping-запрос. Если возможность установления связи с компьютером отсутствует,

появляется сообщение о превышении максимально допустимого времени ответа на запрос (timeout).

Если команда ping для какого-то компьютера выдает сообщение об ошибке, следует проверить с помощью этой команды связь по IP-адресу собственного компьютера, шлюза по умолчанию, а также сервера имен с целью выявления источника ошибок.

Команда tracert

Диагностическая программа предназначена для определения маршрута до точки назначения с помощью посылки в точку назначения эхо-пакетов протокола Internet Control Message Protocol (ICMP) с различными значениями параметра Time-To-Live (TTL). При этом требуется, чтобы каждый маршрутизатор на пути следования пакетов уменьшал эту величину по крайней мере на 1 перед дальнейшей пересылкой пакета, что делает параметр TTL эффективным счетчиком числа промежуточных узлов. Предполагается, что когда параметр TTL становится равен 0, маршрутизатор посылает системе-источнику сообщение ICMP "Time Exceeded". Команда tracert определяет маршрут путем посылки первого эхо-пакета с параметром TTL, равным 1, и с последующим увеличением этого параметра на единицу до тех пор, пока не будет получен ответ из точки назначения или не будет достигнут максимум параметра TTL. Маршрут определяется путем анализа полученных от постоянных маршрутизаторов сообщений ICMP "Time Exceeded". Следует иметь ввиду, что некоторые маршрутизаторы просто сбрасывают пакеты с истекшим временем жизни (то есть с нулевым значением параметра TTL). Такие маршрутизаторы невидимы для команды tracert.

Синтаксис

tracert [-d] [-h максимальное_число_переходов] [-j список_узлов] [-w интервал] [имя_конечного_компьютера]

Параметры

-d

Предотвращает попытки команды tracert разрешения IP-адресов промежуточных маршрутизаторов в имена. Увеличивает скорость вывода результатов команды tracert.

-h максимальное_число_переходов

Задает максимальное количество переходов на пути при поиске конечного объекта. Значение по умолчанию равно 30.

-j список_узов

Указывает для сообщений с эхо-запросом использование параметра свободной маршрутизации в заголовке IP с набором промежуточных мест назначения, указанных в списке_узлов. При свободной маршрутизации успешные промежуточные места назначения могут быть разделены одним или несколькими маршрутизаторами. Максимальное число адресов или имен в

списке - 9. Список_адресов представляет набор IP-адресов (в точечно-десятичной нотации), разделенных пробелами.

-w интервал

Определяет в миллисекундах время ожидания для получения эхо-ответов протокола ICMP или ICMP-сообщений об истечении времени, соответствующих данному сообщению эхо-запроса. Если сообщение не получено в течение заданного времени, выводится звездочка (*). Таймаут по умолчанию 4000 (4 секунды).

имя_конечного_компьютера

Задает точку назначения, указанную IP-адресом или именем узла.

Примечания:

- Чтобы выполнить трассировку маршрута, вывести значение задержки распространения по сети и потерь пакета на каждом маршрутизаторе и узле в пути, используйте команду pathping.

- Эта команда доступна, только если в свойствах сетевого адаптера в объекте Сетевые подключения в качестве компонента установлен протокол Интернета (TCP/IP).

Примеры

Чтобы выполнить трассировку пути к узлу corp7.microsoft.com, введите команду:

tracert corp7.microsoft.com

Чтобы выполнить трассировку пути к узлу corp7.microsoft.com и использовать узлы 10.12.0.1-10.29.3.1-10.1.44.1 для свободной маршрутизации, введите следующую команду:

tracert -j 10.12.0.1 10.29.3.1 10.1.44.1 corp7.microsoft.com

Команда telnet

Telnet - протокол эмуляции терминала, который обеспечивает поддержку удаленного доступа в Интернет

FTP (File Transfer Protocol, или “Протокол передачи данных”) - один из старейших протоколов в Интернет и входит в его стандарты. Первые спецификации FTP относятся к 1971 году. С тех пор FTP претерпел множество модификаций и значительно расширил свои возможности. FTP может использоваться как в программах пользователей, так и в виде специальной утилиты операционной системы.

FTP предназначен для решения задач разделения доступа к файлам на удаленных хостах, прямого или косвенного использования ресурсов удаленных компьютеров, обеспечения независимости клиента от файловых систем удаленных хостов, эффективной и надежной передачи данных.

Обмен данными в FTP происходит по TCP-каналу. Обмен построен на технологии “клиент-сервер”. FTP не может использоваться для передачи конфиденциальных данных, поскольку не обеспечивает защиты передаваемой информации и передает между сервером и клиентом открытый текст. FTP-сервер может потребовать от FTP-клиента аутентификации (т.е. при

присоединении к серверу FTP-пользователь должен будет ввести свой идентификатор и пароль). Однако пароль, и идентификатор пользователя будут переданы от клиента на сервер открытым текстом.

FTP (File Transfer Protocol) представляет собой протокол передачи данных, с помощью которого можно пересылать двоичные и текстовые файлы между компьютерами. В большинстве случаев для обмена данными по протоколу FTP необходимо иметь соответствующие права доступа. Однако имеются так называемые анонимные FTP-серверы, предоставляющие доступ каждому пользователю, например, для загрузки бесплатного программного обеспечения или получения информационных документов. К примеру, на FTP-серверы фирмы Microsoft вы найдете описание ошибок или дополнительную информацию о продуктах этой фирмы.

Алгоритм работы протокола FTP состоит в следующем:

1. Сервер FTP использует в качестве управляющего соединение на TCP порт 21, который всегда находится в состоянии ожидания соединения со стороны пользователя FTP.

2. После того как устанавливается управляющее соединение модуля “Интерпретатор протокола пользователя” с модулем сервера — “Интерпретатор протокола сервера”, пользователь (клиент) может отправлять на сервер команды. FTP-команды определяют параметры соединения передачи данных: роль участников соединения (активный или пассивный), порт соединения (как для модуля “Программа передачи данных пользователя”, так и для модуля “Программа передачи данных сервера”), тип передачи, тип передаваемых данных, структуру данных и управляющие директивы, обозначающие действия, которые пользователь хочет совершить (например, сохранить, считать, добавить или удалить данные или файл и другие).

3. После того как согласованы все параметры канала передачи данных, один из участников соединения, который является пассивным (например, “Программа передачи данных пользователя”), становится в режим ожидания открытия соединения на заданный для передачи данных порт. После этого активный модуль (например, “Программа передачи данных сервера”) открывает соединение и начинает передачу данных.

4. После окончания передачи данных, соединение между “Программой передачи данных сервера” и “Программой передачи данных пользователя” закрывается, но управляющее соединение “Интерпретатора протокола сервера” и “Интерпретатора протокола пользователя” остается открытым. Пользователь, не закрывая сессии FTP, может еще раз открыть канал передачи данных.

Чтобы создать FTP-соединение, выполните следующие действия:

Выполните команду telnet.

В открывшемся окне введите команду open с адресом необходимого FTP-сервера. Например, чтобы установить связь с сервером Microsoft, введите следующую команду: open ftp.microsoft.com

После установления связи с FTP-сервером можно просматривать список файлов и копировать файлы на свой компьютер.

Команды для работы на FTP-сервере:

ls – Позволяет отобразить список файлов. По команде ls –l (маленькая буква «L») отображается подробный список.

cd – позволяет перейти в требуемый подкаталог.

binary – Позволяет включить двоичный режим, необходимый для передачи двоичных данных. Таким образом, перед тем как копировать двоичные файлы следует с помощью команды binary активизировать двоичный режим. По умолчанию включен режим ASCII.

ascii – Позволяет активизировать текстовый режим.

get – Позволяет скопировать заданный файл на свой компьютер.

disconnect – Позволяет завершить сеанс связи с FTP-сервером без завершения работы программы.

quit – Позволяет завершить сеанс связи с FTP-сервером с завершением работы программы.

С полным списком команд программы FTP можно познакомиться в справочной системе Windows.

Команда ARP

Для определения локального адреса по IP-адресу используется протокол разрешения адреса Address Resolution Protocol, ARP. Протокол ARP работает различным образом в зависимости от того, какой протокол канального уровня работает в данной сети - протокол локальной сети (Ethernet, Token Ring, FDDI) с возможностью широковещательного доступа одновременно ко всем узлам сети, или же протокол глобальной сети (X.25, Frame relay), как правило не поддерживающий широковещательный доступ. Существует также протокол, решающий обратную задачу - нахождение IP-адреса по известному локальному адресу. Он называется реверсивный ARP - RARP (Reverse Address Resolution Protocol) и используется при старте бездисковых станций, не знающих в начальный момент своего IP-адреса, но знающих адрес своего сетевого адаптера.

В поле типа сети для сетей Ethernet указывается значение 1. Поле типа протокола позволяет использовать пакеты ARP не только для протокола IP, но и для других сетевых протоколов. Для IP значение этого поля равно 080016.

Длина локального адреса для протокола Ethernet равна 6 байтам, а длина IP-адреса - 4 байтам. В поле операции для ARP запросов указывается значение 1 для протокола ARP и 2 для протокола RARP.

Узел, отправляющий ARPP-запрос, заполняет в пакете все поля, кроме поля искомого локального адреса (для RARP-запроса не указывается искомый IP-адрес). Значение этого поля заполняется узлом, опознавшим свой IP-адрес.

Отображение и изменение используемой протоколом ARP таблицы соответствия адресов IP и физических адресов.

Формат команды:

ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

-a Вывод текущих записей таблицы ARP путем опроса текущих данных протокола. Если указан адрес inet_addr, то адреса IP и физические выводятся только для указанного компьютера. Если протокол ARP используется несколькими сетевыми интерфейсами, то выводятся записи из каждой таблицы .

-g Аналог –a.

inet_addr Задание адреса IP.

-N if_addr Вывод текущих записей таблицы ARP для сетевого интерфейса, определяемого параметром if_addr.

-d Удаление узла, определяемого параметром inet_addr.

-s Добавление узла и связывание адреса IP inet_addr с физическим адресом eth_addr. Физический адрес задается с помощью 6 шестнадцатеричных чисел, разделяемых дефисами. Запись является постоянной.

eth_addr Задание физического адреса.

if_addr Необязательный параметр, указывающий адреса IP интерфейса, для которого следует изменить таблицу адресов. Если параметр не задан, используется первый доступный интерфейс.

Например:

arp –a … Выводит таблицу arp.

arp –s 176.16.1.400 00-aa-00-62-c6-09 … Добавляет статическую запись.

Команда route Управление таблицами маршрутизации в сети. Эта команда доступна только после установки поддержки протокола TCP/IP.

Формат команды:

route [-f] [-p] [команда [компьютер] [mask маска] [шлюз] [metric мера]]

Параметры:

-f Удаление записей о всех шлюзах. Если используется в сочетании с одним из других ключей, вначале удаляются соответствующие записи, а затем выполняются действия, заданные другим ключом.

-p При использовании с командой ADD обеспечивает сохранение маршрутов при перезагрузке системы. По умолчанию маршруты не сохраняются при перезапуске системы. При использовании с командой PRINT выводит на экран список зарегистрированных постоянных маршрутов. При использовании с другими командами, ключ игнорируется, и команды работают с соответствующим постоянным маршрутом.

команда

Одна из четырех команд:

Команда Действие

print Вывод маршрута

add Добавление маршрута

delete Удаление маршрута

change Изменение существующего маршрута

компьютер

Компьютер, на который посылается команда.

mask маска Задает маску подсети, которая ассоциируется с данным маршрутом. Если маска не задана, используется 255.255.255.255.

шлюз Задает шлюз.

Все символические имена, используемые в параметрах компьютер и шлюз, ищутся в базах данных сетей и компьютеров, находящихся в файлах NETWORKS и HOSTS, соответственно. Для команд print и delete могут быть использованы символы подстановки для параметров компьютер и шлюз, или может быть опущен параметр шлюз.

metric мера Задает целочисленный параметр меры (от 1 до 9999), которая может быть использован для вычисления самого быстрого, самого доступного или наиболее дешевого маршрута.

Другие команды

nbtstat – Позволяет отобразить статистику работы и перечень текущих соединений по протоколу NBT (NetBIOS через TCP/IP).

netstat – Позволяет отобразить перечень текущих TCP/IP-соединений.

Задание

1. Ознакомиться с указанными сетевыми утилитами.

2. Выполнить каждую команду с максимально возможным употреблением параметров.

3. Составить отчет по лабораторной работе.

3.4 Методические указания по выполнению задания

Для работы с сетевыми утилитами вам нужно запустить” командную строку” 1.В Windows нажать кнопку «Start»(Пуск), в меню «Start»(Пуск), выбрать пункт «Run»(Выполнить).

После этого появится диалоговое окно «Run»(Выполнить).В поле «Open»(Открыть) введите “Cmd” нажмите кнопку ок.

Появится окно командной строки.

В этом окне вы вводите команды.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 2

Исследование установки и начальной настройки систем

Цель работы: Ознакомиться с начальными настройками системы

Теоретическая часть:

Установка и первичная настройка Windows Server 2012

Инсталляция Windows Server 2012.

Среди операционных систем Windows XP является наиболее распространенной. Поэтому рассмотрим последовательность развертывания системных программных средств на примере этой системы. Для загрузки Windows XP необходим следующий минимальный набор файлов, расположенных: а) в корневом каталоге загрузочного диска (ntldr; boot.ini, bootsect.dos, NTDETECT.C); б) в системном подкаталоге Windows/system32 (ntoskrnl.exe, hal.dll, разделы реестра System); в) в системном подкаталоге /system32/drivers (необходимые драйверы устройств).

Процесс загрузки компьютера начинается с процедуры начального тестирования оборудования (^ POST – Power-On Self Test). Код, выполняющий POST, зашит в базовой системе ввода-вывода (BIOS) каждого компьютера, и именно ему передается управление при включении питания. Если в процессе тестирования обнаруживаются какие-либо ошибки, то BIOS генерирует коды ошибок (POSTcodes), которые отличаются для BIOS разных производителей, и звуковые коды. Если процедура POST завершается успешно, то BIOS передает управление главной загрузочной записи (MBR – Master Boot Record) первичного жесткого диска системы, чем завершается первая «аппаратная» стадия загрузки компьютера (весь процесс зависит только от аппаратуры компьютера, но не от установленного программного обеспечения).

На второй стадии загрузочная запись, оперируя данными о разбиении жесткого диска на логические тома, передает управление исполняемому коду, расположенному в загрузочном секторе. В операционной системе Windows XP этим кодом является загрузчик операционной системы ntldr. Загрузчик переходит в защищенный режим работы и производит необходимые для успешного функционирования в этом режиме манипуляции с памятью. Кроме функций, позволяющих работать с памятью, ntldr имеет также несколько модулей, позволяющих работать с некоторыми другими базовыми ресурсами системы, в первую очередь с файловой системой. Все другие действия выполняются с помощью вызова прерываний BIOS.

После первичной инициализации загрузчик предоставляет пользователю возможность выбрать операционную систему, которая будет загружена из списка систем установленных на компьютере. С этой целью ntldr выводит на экран надпись: «OS Loader V5.0» и приглашение выбрать операционную систему. Сообщение выводится только в том случай если в файле boot.ini зарегистрировано более одной операционной системы. После выбора операционной системы загрузчик запускает файл NTDETECT.COM.

Этот компонент считывает из CMOS-памяти системную дату и время и производит поиск и распознавание аппаратных средств, подключенных в данный момент к компьютеру. Завершив работу, NTDETECT возвращает управление и собранную им информацию обратно в ntldr.

Далее загружается и инициализируется ядро операционной системы ntoskrnl.exe и уровень абстрагирования от оборудования hal.dll. При своей инициализации ядро производит ряд действий в следующей последовательности:

-Инициализация диспетчера памяти.

-Инициализация диспетчера объектов.

-Установка системы безопасности.

-Настройка драйвера файловой системы.

Загрузка и инициализация диспетчера ввода-вывода (обычно самая длительная фаза).

Загрузка системных сервисов, которые реализуют взаимодействие с пользователем.

Загрузка Session Manager (Smss.exe), который:

-переключает Windows из текстового режима в графический;

-запускает менеджер входа в систему Logon Manager (systemroot \System32\Winlogon.exe);

-создает дополнительные файлы виртуальной памяти;

-если установлены новые программы и/или драйверы, то спросит перезагрузить систему.

-Менеджер входа в систему Logon Manager (Winlogon.exe) запускает подсистему сервисов (Services.exe) и локальную систему безопасности (Local Security Authority, Lsass.exe) и делает возможным комбинацию клавиш CTRL+ALT+DEL, чтобы показать логин скрин.

-Загруженная операционная система обеспечивает следующие системные приложения1:

Csrss.exe – данный модуль предназначен, главным образом, для организации взаимодействия между компьютером и пользователем. Он является частью подсистемы Win32 и поэтому этот процесс нельзя закрыть в менеджере задач. Csrss (client/server run-time subsystem – клиент /серверная подсистема) отвечает за консольные приложения, создание/удаление потоков и за 16-битную виртуальную среду MS-DOS.

Уже после загрузки операционной системы пользователь, чтобы доказать, что он тот, за кого себя выдает, должен пройти процедуру аутентификации, то есть ввести собственное регистрационное имя (логин) и пароль. Данные действия при пониженных требованиях к безопасности могут быть настроены по умолчанию. Процедура подключения к системе позволяет определить, кем является пользователь и обладает ли он правом входа и работы с системой. При выполнении этой процедуры службой WinLogon в системе происходят следующие события:

процесс WinLogon отображает на экране фон рабочего стола (к этому моменту объект рабочего стола уже создан, но еще не отображается), а также приглашение к вводу пользователем логина и пароля; введенные данные передаются подсистеме безопасности;

подсистема безопасности обращается к базе данных ^ SAM (Security ccounts Manager) и проверяет, обладает ли пользователь полномочиями работы с системой;

Базовая Система Ввода Вывода

Базовая Система Ввода Вывода (BIOS) – часть программного обеспечения вычислительной системы, поддерживающая управление адаптерами внешних устройств, экранные операции, тестирование, начальную загрузку и установку операционной системы. BIOS – это стандартный интерфейс, обеспечивающий переносимость операционной системы между компьютерами с одинаковым микропроцессором. BIOS хранится в постоянном запоминающем устройстве компьютера. Управление устройствами осуществляется через механизм прерываний. Различают следующие прерывания:

-аппаратные прерывания – инициируются аппаратными средствами;

-логические прерывания – инициируются микропроцессором, нестандартные ситуации в работе микропроцессора;

-программные прерывания – инициируются программным обеспечением.

При включении компьютера автоматически загружается и выполняется специальная программа ^ POST(Power-On Self-Test) из состава BIOS. Эта программа производит самопроверку и тестирование при загрузке:

-проверка переключателей и CMOS-памяти на системной (материнской) плате, определение оборудования, которое подключено к компьютеру;

-тестирование оперативного запоминающего устройства;

-выполняет действия по загрузке операционной системы (загрузка в оперативную память и запуск Блока Начальной Загрузки операционной системы);

-выполняет другие специфические действия по подготовке компьютера и дополнительного оборудования к работе.

BIOS является своеобразной программной оболочкой самого нижнего уровня вокруг аппаратных средств компьютера, которая реализует доступ к аппаратным средствам компьютера через механизм прерываний. Структура BIOS включает две главные части:

Главный исполняемый код – состоит из нескольких модулей и хранится в виде архива LHA, как правило, используются следующие названия для модулей архива

original.tmp – главная часть размером 128k, в которой происходит инициализация компьютера и находится подпрограмма BIOS Setup;

awardext.rom – расширение главной части, содержит подпрограмму вывода конфигурации;

awardepa.bin – картинка Energy Star;

другие встречающиеся части: cpucode.bin – таблица микрокодов для Intel-процессоров (PPro, P2/P3/P4, Celeron); acpitbl.bin – подпрограмма поддержки ACPI и др.

Доступ к BIOS Setup (программе настройки) осуществляется нажатием определенных комбинаций клавиш, обычно нажатием клавиши ^ Delete в момент начальной загрузки системы. Структура меню программы настроек и название блоков в каждой из версий BIOS могут отличаться, однако основные фразы меню могут повторяться или быть схожими. Программа настройки BIOS разделена на определенные блоки, каждый из которых позволяет настроить соответствующие группы параметров. Опции BIOS Setup:

предупреждение отказов жестких дисков – все современные жесткие диски поддерживают технологию S.M.A.R.T., позволяющую заранее оповестить о потенциальных проблемах с дисками и их возможных отказах;

антивирусная защита – попытка аппаратной защиты от вирусов путем перезаписи загрузочных секторов дисков, практически опция не используется;

центральный процессор – опции, отвечающие за функционирование процессора, за исключением установки частот и напряжений питания;

параметры загрузки – определение порядка и скорости загрузки;

клавиатура и мышь – устанавливает возможность установить некоторые режимы функционирования клавиатуры и мыши;

пароли – используются для защиты от несанкционированной модификации значений опций в BlOS Setup и от нежелательного использования компьютера третьими лицами.

затенение областей памяти – перенос в оперативную память из содержимого ^ ПЗУ интеллектуальных карт расширения, имеющих свой BIOS; поскольку доступ к оперативной памяти требует меньше времени, чем обращение непосредственно к ПЗУ с BIOS карты, то и обмен данными происходит быстрее;

настройка режимов работы оперативной памяти – в зависимости от того, правильно ли выполнены настройки оперативной памяти, зависит скорость и надежность работы компьютера;

дополнительные возможности чипсета при работе с памятью – используется для настройки режимов обращения к памяти со стороны других устройств;

функционирование шины PCI – играют важную роль в работе компьютера, так как указание неверных значений способно привести к нестабильной работе карт расширения, конфликтам между ними;

режимы работы шины ^ AGP и видеокарты – в большинстве случаев видеокарта подключается к шине AGP;

параметры кэширования – перенос данных из медленной памяти в более быструю память (в данном случае перенос данных в оперативную память);

дополнительные возможности BIOS – часть производителей материнских плат предлагают дополнительные опции, расширяющие возможности материнской платы;

работа интегрированных устройств – чипсет сам содержит контроллеры некоторых устройств, таких как: жесткие диски и приводы чтения компакт-дисков, порты, дисководы и т.п., в дополнение к этому производители часто размещают на материнских платах интегрированные устройства, например, звуковые карты;

распределение ресурсов – в большинстве случаев распределение ресурсов происходит автоматически, но если компьютер «перегружен» картами расширения, может потребоваться и ручное назначение прерываний и каналов прямого доступа к памяти;

ручной контроль напряжений и частот – некоторые материнские платы позволяют вручную изменять напряжения, подаваемые на отдельные компоненты компьютера, указывать частоту системной шины, множитель процессора и т.п., но пользоваться ими следует очень осторожностью, так как при выставлении неверных значений компьютер может не запуститься.

Задание

1. Ознакомиться с установкой и начальных настройках системы
2. Составить отчет по лабораторной работе.
3. Методические указания по выполнению задания

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 3

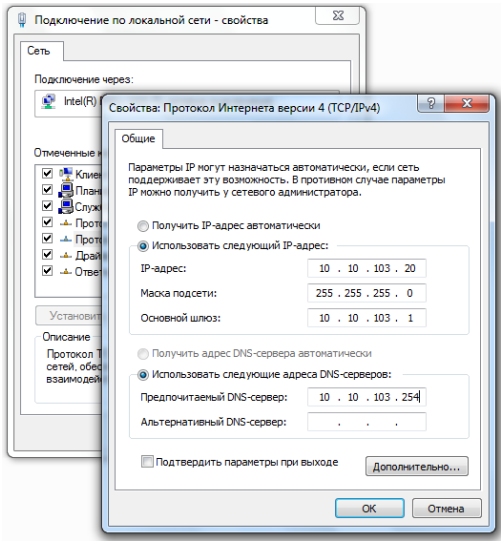
Исследование адресации узлов в IP-сетях

Цель работы: Ознакомиться с адресацией узлов в IP-сетях

Теоретическая часть:

Адресация в IP сети В IP сетях используют три типа: физические адреса узлов – MAC адреса (физический уровень); сетевые адреса – IP адреса (сетевой/транспортный уровень); символьные адреса – DNS (Domain Name System) имена (прикладной уровень) или доменные имена используемые для удобства запоминания. Связь между DNS именем и IP адресом устанавливается службой DNS. Например, для IP адреса Web сервера нашего факультета 212.46.206.2 закреплено имя www.fem-sut.spb.ru.. Остановимся на полном сетевом IPv4 адресе, который представляет собой три 4-х байтовых числа: адрес. Например, 192.168.3.11 маска. Например, 255.255.255.0 шлюз. Например, 192.168.3.1 Используется несколько форм записи байтов IP адреса: Десятичная нотация (наиболее употребительная) – значения чисел в каждом байте записываются как десятичные числа от 0 до 255=28-1 включительно. Двоичная нотация - значения чисел в каждом байте записываются как двоичные числа от 0000 0000 до 1111 1111 включительно. Шестнадцатиричная нотация - значения чисел в каждом байте записываются как шестнадцатиричные числа от 00 до FF включительно. Маска служит для отделения в IP адресе номера сети от номера узла. Для сокращения записей иногда маска обозначается количеством единиц в старших разрядах, например, для адреса 192.168.3.11 и маски 255.255.255.0, что в двоичной форме соответствует адресу 1100 0000.1010 1000.0000 0011.0000 0011 и маске 1111 1111.1111 1111.1111 1111.0000 0000, можно записать 192.168.3.11/24. Смысл маски IP адреса можно понять, рассмотрев действия узла при приёме пакета. В принятом пакете на адрес назначения накладывается маска и определяется номер сети назначения. Термин «накладывается» означает побитовое логическое умножение (операция «И») 4-х байтового IP адреса на 4-е байта маски. Например, IP адрес 192.168.3.187 (1100 0000.1010 1000.0000 0011.1011 1011) маска 255.255.255.240 (1111 1111.1111 1111.1111 1111.1111 0000) результат наложения (номер сети) 192.168.3.176 (1100 0000.1010 1000.0000 0011.1011 0000) Если номер сети не «наш», пакет игнорируется. Если сеть «наша», то выполняется следующий шаг. Проверяется: совпадение своего номера узла и номера узла назначения или наличие признака широковещательной рассылки. Адрес широковещательной рассылки имеет значения 1 в битах, относящихся к номеру узла (хоста). Для примера из п.1 это 192.168.3.191 (1100 0000.1010 1000.0000 0011.1011 1111)

1.Ручная настройка.



2. Автоматическая настройка

A. Динамическое распределение IP-адресов — DHCP

DHCP (англ. Dynamic Host Configuration Protocol — протокол динамической конфигурации узла) — это сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP. Для этого компьютер обращается к специальному серверу, называемому сервером DHCP. Сетевой администратор может задать диапазон адресов, распределяемых среди компьютеров. Это позволяет избежать ручной настройки компьютеров сети и уменьшает количество ошибок. Протокол DHCP используется в большинстве крупных сетей TCP/IP.

Алгоритмритм разделения сети на подсети

I. Определение маски подсети

1. Необходимо определить число разрядов в идентификаторе подсети – S. Используется следующее правило:

N = 2^S (два в степени S)

N – число подсетей в общей сети

S – число разрядов в идентификаторе подсети

Делим сеть на две подсети:

2=2^1 => S = 1

2. Запишите S единиц подряд и добавьте справа столько 0, чтобы общее количество разрядов соответствовало разрядности идентификатора хоста общей сети (для сети класса A – 8 р; для сети класса B – 16 р и т.д.)

Сеть класса A: 10000000 => 128

Сеть класса B: 10000000.00000000 => 128.0 3.

3. Запишите полученное число на месте ID-хоста в маске, определяющей общую сеть.

Сеть класса A: 255.255.255.128 => /25

Сеть класса B: 255.255.128.0 => /1

II. Определение адресов подсетей

Адрес сети (подсети) – адрес в котором ID-хоста заменяется нулями. Для задания идентификаторов подсетей используется то же число разрядов S, что и для соответствующей маски

Запишите все двоичные числа, образованные изменением S разрядов и добавьте справа столько 0, чтобы общее количество разрядов соответствовало числу разрядов в ID-хоста маски подсети.

Запишите полученное число на месте ID-хоста в адресе общей сети.

Сеть класса A: 0 0000000 => 0
1 0000000 => 128

Подсети: W.X.Y.0
W.X.Y.128

Сеть класса B: 0 0000000.00000000 => 0.0
1 0000000.00000000 => 128.0

Подсети: W.X.0.0
W.X.128.0

III. Определение диапазонов адресов для узлов подсети

Начало диапазона – увеличенный на 1 адрес подсети

Конец диапазона – уменьшенный на 2 адрес следующей возможной подсети (все 0 в адресе хоста – адрес сети; все 1 в адресе хоста – широковещание)

Сеть класса A: W.X.Y.1 - W.X.Y.126
W.X.Y.129 - W.X.Y.254

Сеть класса B: W.X.0.1 - W.X.127.254
W.X.128.1 - W.X.255.254

IV. Определение количества хостов подсети

1. Запишите маску подсети и определите число разрядов в идентификаторе узла – H

Сеть класса A: 255.255.255.128 => /25 => H = 7

Сеть класса B: 255.255.128.0 => /17 => H = 15

2. Число возможных адресов – 2^H

3. Число доступных адресов – 2^H-2 (все 0 в адресе хоста – адрес сети; все 1 в адресе хоста – широковещание)

Адресация хостов в сети.

Каждый компьютер в сети имеет уникальное имя.

1.В IP-сетях в качестве уникального имени хоста используется IP-адрес.

2. Локальный (аппаратный) адрес или MAC-адрес.

- Адресс, присвоенный сетевому адаптеру на заводе изготовителе. (MAC – Media Access Control – управление доступом к среде). Слово локальный означает «действующий не во всей составной сети, а лишь в пределах локальной сети (подсети). Внутри ЛВС хосты устанавливают связь друг с другом, используя эти адреса (канальный уровень OSI).

3. DNS-имя.

DNS (Domain Name System) – доменная система имен. Реализуется в виде иерархического пространства имен, в котором имя представляет собой последовательность простых символьных имен, разделенных точками.

DNS (Domain Name System) – это распределенная база данных, которая распределена между специальными компьютерами сети – DNS-серверами. Домен – группа сетевых хостов, имеющая уникальное имя. DNS-сервер создается в каждом домене. DNS-сервер хранит доменные имена и соответствующие им IP-адреса.

4. NetBIOS-имя (плоское имя).

Имя, присваиваемое компьютеру внутри локальной сети. Состоит из последовательности символов, не разделенных на части. Используется только для связи внутри локальной сети (например, для доступа к общим каталогам и принтерам).

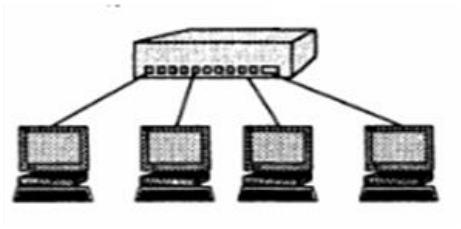
Разрешение имен.

Разрешение имени – установление однозначного соответствия (отображение) между именами разного типа.

1. Отображение IP-адресов на MAC-адреса.

Каждый сетевой интерфейс (сетевой адаптер) имеет IP-адрес и MAC-адрес. Для определения MAC-адреса по IP-адресу используется протокол ARP (Address Resolution Protocol). Протокол ARP поддерживает для каждого сетевого адаптера или маршрутизатора таблицу ARP. Первоначально, при включении компьютера или маршрутизатора в сеть, все его таблицы маршрутизации пусты. В них накапливается информация в ходе работы сети.

IP-адрес	MAC-адрес	Тип записи
194.85.135.65	00E0F77F1920	Динамический
194.85.135.75	008048EB7E60	Динамический
194.85.60.21	008048EB7567	Статический



Пусть IP-протокол узла А направляет пакет узлу В с адресом IP1.

Для решения этой задачи:

- Протокол IP обращается к протоколу APR

«Какой MAC-адрес имеет узел с адресом IP1?»

- Работа ARP начинается с просмотра APR-таблицы. Предположим, что в ней отсутствует запись об адресе IP1

- Протокол ARP формирует ARP-запрос и рассылает в сеть всем хостам (широковещание) сети.

- Хосты направляют запрос своему протоколу ARP. Он сравнивает полученный в запросе адрес IP1 со своим IP-адресом.

- ARP, который констатировал совпадение, формирует ARP-ответ, в котором указывает свой MAC-адрес. Широковещания здесь нет, т.к. в ARP-запросе был указан MAC-адрес отправителя.

Зона ARP-запросов ограничивается локальной сетью, т.к.

маршрутизаторы не передают эти запросы в другие сети.

Задание

1. Ознакомиться с адресацией узлов в IP-сетях
2. Составить отчет по лабораторной работе.
3. Методические указания по выполнению задания

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 4

Исследование планирования пространства имен службы каталогов

Цель работы: Научиться планировать, устанавливать и конфигурировать службу каталогов Active Directory.

Теоретический материал и задания.

Обзор Active Directory. Active Directory — это служба каталогов Windows 2000 Server. Active Directory расширяет функциональность предыдущих служб каталогов Windows, включает новые возможности и обеспечивает безотказную работу в сетях любого размера: от одного сервера с несколькими сотнями объектов, до тысяч серверов с миллионами объектов. Множество новых функций Active Directory облегчают навигацию и управление большими объемами информации.

Службы Active Directory обеспечивают иерархическое представление содержания каталога, расширяемость, масштабируемость и соблюдение правил безопасности. Active Directory объединяет концепцию пространства имен Интернета со службой каталога ОС. LDAP - основной протокол Active Directory — позволяет централизованно работать с каталогами различных ОС, объединяя множество пространств имен. Схема содержит формальное описание содержания и структуры хранилища Active Directory, включая все атрибуты, классы и свойства классов. Глобальный каталог — центральное хранилище информации об объектах в дереве или лесе — выполняет роль службы и физического хранилища, содержащего реплику ряда атрибутов каждого объекта в хранилище Active Directory. Как и все службы каталога, Active Directory — это прежде всего пространство имен; каждый объект в хранилище Active Directory идентифицируется по имени. Структура Active Directory включает несколько основных компонентов: схему, модели данных, безопасности и администрирования. Доступ к Active Directory осуществляется по сетевым протоколам, определяющим форматы сообщений и порядок взаимодействия клиентов с сервером. Архитектура Active Directory состоит из трех уровней, нескольких интерфейсови протоколов, совместно предоставляющих службы каталога.

Active Directory позволяет централизованно администрировать все опубликованные ресурсы: файлы, периферийные устройства, хост-соединения, базы данных, доступ к Интернету, учетные записи пользователей, службы и другие объекты. Active Directory применяет в качестве службы поиска реалиюванную в Интернете систему доменных имен (Domain Name System, DNS), упорядочивающую объекты в доменах в иерархию организационных подразделений (ОП), и позволяет объединить несколько доменов в древовидную структуру. Это также помогает упростить администрирование за счет отказа от иерархии основной/резервный контроллер домена, применявшейся в Windows NT Server, поскольку в Active Directory все

контроллеры равноправны. Изменения, внесенные на любом контроллере домена, будут скопированы на все остальные контроллеры.

Перед реализацией сетевой среды на базе Windows 2000 Вы должны решить, как внедрить Active Directory. При планировании нужно учесть структуру и деятельность предприятия: физическое размещение офисов, возможность расширения и реорганизации и порядок доступа к сетевым ресурсам. Сначала планируется пространство имен DNS. Включая иерархию домена, глобальный каталог, доверительные отношения и репликацию. Кроме того, пространство имен включает организационные подразделения (ОП), структуру которых также следует учесть на этапе планирования, В одиночном домене объекты пользователей и ресурсов можно упорядочить в иерархию ОП для отражения структуры компании. Надо спланировать и границы сайтов — это упростит управление репликацией и сократит трафик регистрационных данных пользователей между подразделениями.

Подобно DNS, в основе пространства имен Active Directory лежит полное имя домена высшего уровня информационной системы предприятия, состоящей из доменов Windows 2000, контроллеров доменов, ОП, доверительных отношений и деревьев доменов. Кроме того, важно сразу решить, будут ли одинаковы внутреннее (защищенное брандмауэром) и внешнее (за его пределами) пространство имен. Иначе говоря, будет ли пространство имен Active Directory соответствовать пространству имен DNS (как правило, имени домена в Интернете), которое, возможно, уже определено для Вашей организации?

Выбрав модель взаимодействия внутреннего и внешнего пространств имен, надо учесть и другие факторы, например объем трафика репликации по ГВС и потенциальные изменения структуры предприятия. Помимо возможности создания леса в Windows 2000, администраторы должны быть готовы оперативно корректировать архитектуру пространства имен с минимальными издержками и без остановки работы сети. Цель — получить масштабируемую архитектуру, способную адаптироваться к изменениям, обеспечивающую непрерывный доступ к внутренним и внешним ресурсам и защиту данных.

Архитектура пространства имен должна отражать структуру предприятия и одновременно обеспечивать степень административной детализации, необходимую для эффективного управления корпоративной и глобальной сетью посредством Active Directory. Соблюсти эти условия позволяет наличие трех уровней доменов:

корневой домен; домен первого уровня; домен второго уровня.

Эта структура обеспечивает гранулярную топологию репликации и позволяет при необходимости ограничить полномочия нижестоящих администраторов.

Внедрение Active Directory. Для установки Active Directory на компьютер Windows 2000 Server применяется мастер Active Directory Installation (Мастер установки Active Directory). Этот мастер также позволяет

добавить контроллер в существующий домен, создать первый контроллер домена, дочерний домен и новое дерево доменов. При установке Active Directory автоматически создаются база данных, файлы ее журнала и общий системный том. БД каталога находится в файле Ntds.dit, который является хранилищем Active Directory. Общий системный том — это структура каталога, существующая на всех контроллерах домена Windows 2000. Он хранит сценарии и некоторые объекты групповой политики для текущего домена и для предприятия в целом. Домен может работать в смешанном или основном режиме. При первоначальной установке или обновлении контроллера домена до Windows 2000 Server контроллеры запускаются в смешанном режиме. Если все контроллеры домена переведены на Windows 2000 Server и Вы больше не собираетесь добавлять к домену контроллеры на базе предыдущих версий Windows, переведите домен в основной режим.

Мастер Active Directory Installation (Мастер установки Active Directory) позволяет:

- добавить контроллер домена к существующему домену;
- создать первый контроллер нового домена;
- создать новый дочернеий домен;
- создать новое дерево доменов.

Для запуска мастера Active Directory Installation раскройте меню Start\Programs\Administrative Tools (Пуск\Программы\Администрирование) и щелкните ярлык Configure Your Server (Настройка сервера). На левой панели открывшегося окна щелкните ссылку Active Directory, прокрутите содержимое окна вниз и выберите ссылку вызова мастера. Или запустите утилиту dcpromo.exe из окна Run или из командной строки. В любом случае откроется окно мастера, который поможет Вам установить Active Directory на компьютер и создать контроллер домена.

При установке Active Directory Вы сможете выбрать: добавить ли новый контроллер к существующему домену, или создать первый контроллер для нового домена.

Задание 1: повысьте изолированный сервер до контроллера домена

С помощью программы dcpromo.exe установите Active Directory и службу DNS на изолированный сервер (Server01) и превратите его в контроллер и DNS-сервер нового домена.

1. Зарегистрируйтесь на Server01 как Administrator (Администратор) с паролем password.

2. Если откроется окно Windows 2000 Configure Server (Настройка сервера Windows 2000), закройте его, так как для выпотнения этого упражнения Вы используете утилиту dcpromo.exe.

3. Вставьте установочный компакт-диск Windows 2000 Server в привод CD-ROM на Server01. Компакт-диск необходим для установки службы DNS в ходе работы dcpromo.exe.

4. Если сработает программа автозапуска, закройте ее окно, щелкнув ссылку Exit (Выход).

5. В меню Start (Пуск) выберите команду Run (Выполнить).

6. В диалоговом окне Run (Запуск программы) наберите dcpromo.exe и щелкните кнопку ОК. Откроется окно мастера Active Diiectory Installation (Мастер установки Active Directory).

7. Щелкните кнопку Next (Далее).Откроется окно Domain Controller Type (Тип контроллера домена).

8. Выберите Domain Controller For New Domain (Контроллер домена в новом домене) и щелкните кнопку Next (Далее). Откроется окно Create Tree Or Child Domain (Создание дерева или дочернего домена).

9. Убедитесь, что выбран переключатель Create A New Domain Tree (Создать новое доменное дерево) и щелкните кнопку Next (Далее). Откроется окно Create Or Join Forest (Создание леса или присоединение к лесу).

10. Щелкните переключатель Create A New Forest Of Domain Trees (Создать новый лес доменных деревьев) и щелкните Next (Далее). Откроется окно New Domain Name (Имя DNS-домена).

11. В поле Full DNS Name For The N^w Domain введите microsoft.com и щелкните кнопку Next (Далее). Откроется окно NetBIOS Domain Name (NetBIOS-имя домена).

12. Убедитесь, что в поле Domain NetBIOS Name (NetBIOS-имя домена) выведено MICROSOFT и щелкните кнопку Next (Далее). Откроется окно Database And Log Locations (Местоположение базы данных и журнала).

13. Убедитесь, что для размещения базы данных и протокола выбран путь C:\Winnt\ Ntds и щелкните кнопку Next (Далее). Откроется окно Shared System \blume (Общий доступ к системному тому).

14. Изучите информацию в этом окне и убедитесь, что для размещения SYSVOL указан путь C:\WINNT\SYSVOL.

15. Щелкните кнопку Next (Далее). Появится сообщение, что мастер не может связаться с DNS-сервером, обрабатываю-

щим имя microsoft.com.

16. Щелкните кнопку ОК. Поскольку мастер не нашел DNS-сервер, откроется окно Configure DNS (Настройка DNS).

17. Убедитесь, что выбран переключатель Yes, Install And Configure DNS On The Corhputer (Recommended) (Да, автоматически установить и настроить DNS) и щелкните кнопку Next (Далее). Откроется окно Permissions (Разрешения).

18. Первоначально контроллер домена запустится в смешанном режиме, поэтому убедитесь, что выбран переключатель Permissions Compatible With Pre-Wmdows 2000 Servers (Разрешения, совместимые с серверамипред-Windows 2000) и щелкните кнопку Next (Далее). Откроется окно Directory Services Restore Mode Administrator Password (Пароль администратора для режима восстановления).

19. Изучите информацию в этом окне, а затем наберите password в обоих полях и щелкни те кнопку Next (Далее). Откроется окно Summary (Сводка), представляющее список выбранных Вами параметров установки.

20. Изучите содержание этого окна и щелкните кнопку Next (Далее). Появится индикатор хода установки Configuring Active Directory (Идет настройка Active Directory). Этот процесс займет несколько минут. Проверьте, вставлен ли установочный компакт диск Windows 2000 Server в Server01 — он понадобится для установки службы DN S.

21. Когда откроется окно Completing The Active Directory Installation Wizard (Завершение работы мастера установки Active Directory), выньте компакт-диск из привода, щелкни те кнопку Finish (Готово) и перезагрузите компьютер. Первый запуск Windows 2000 Server в роли контроллера домена проходит медленнее обычного.

Администрирование Active Directory. После установки Active Directory Вы можете управлять объектами, хранимыми в каталоге. Перед добавлением объектов в Active Directory надо создать ОП, где они будут содержаться. Вы можете создать ОП на уровне домена, контроллера домена или внутри другого ОП; при этом Вы должны обладать соответствующими разрешениями. Управление объектами Active Directory включает их поиск, изменение, перемещение и удаление. Эти задачи вы полняются в оснастке Active Directory Users And Computers (Active Directory — пользователи и компьютеры), ярлык которой расположен в программной группе Administrative Tools (Администрирование). Еще один аспект администрирования Active Directory - управление доступом к объектам каталога. Разрешения Active Directory обеспечивают защиту ресурсов, позволяя контролировать доступ к индивидуальным объектам и их атрибутам, а также вид доступа. Кроме того, Вы можете делегировать полномочия администрирования объектов другим лицам для выполнения административных задач в отношении указанных объектов. Ниже приведены рекомендации по администрированию Active Directory:

В крупных организациях заранее согласовывайте структуру Active Directory с другими администраторами. Вы сможете переместить объекты и позже, но это потребует дополнительных усилий.

При создании таких объектов Active Directory, как User, заполняйте все атрибуты, важные для Вашей организации. Чем больше атрибутов определено, тем шире возможности поиска.

Осторожно аннулируйте разрешения. При правильном назначении разрешений Вам, возможно, никогда не понадобится их отменять. Чаще всего аннулирование разрешений свидетельствует об ошибках группирования объектов.

Всегда проверяйте, чтобы минимум один пользователь имел разрешение Full Control (Полный доступ) для всех объектов Active Directory, иначе объекты могут оказаться недоступны.

Убедитесь, что уполномоченные пользователи ответственно относятся к возложенным на них функциям и способны пранильно их выполнять. В конце концов, как администратор, именно Вы отвечаете за все изменения в системе, и

если пользователи, которым Вы доверили выполнение ряда задач в их сети, не справляются, отвечать за их ошибки придется Вам.

Инструктируйте уполномоченных пользователей. Убедитесь, что они понимают важность их работы и умеют выполнять задачи администрирования.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 5

Исследование управления пользователями и группами

Цель работы: Ознакомиться с управлением пользователями и группами

Теоретическая часть:

Администратор безопасности компьютера

Любой пользователь компьютера, при соблюдении перечисленных ниже условий, может быть назначен администратором безопасности компьютера по умолчанию:

· пользователь должен обладать всеми привилегиями на администрирование системы защиты, и для него должен быть включен режим запроса пароля при входе в систему.

· пользователь, являющийся администратором по умолчанию, не может быть удален из списка пользователей компьютера.

Для выбора администратора безопасности компьютера необходимо:

1. Вызвать на экран окно управления общими параметрами.

2. Активизировать диалог «Дополнительно»:

Рис. 1. Диалог «Дополнительно»

3. Выбрать в списке «Администратор по умолчанию» нужное имя пользователя.

4. Нажать кнопку «ОК».

2. Пользователи

В системе Secret Net каждому реальному пользователю компьютера ставится в соответствие объект системы защиты - «Пользователь». Далее под управлением пользователем будем понимать управление этим объектом.

Для создания (регистрации) или удаления пользователя необходимо обладать привилегиями на администрирование группы «Пользователи и группы пользователей».

Создание пользователя

Чтобы включить нового пользователя в состав пользователей компьютера, необходимо создать объект «Пользователь».

Для создания пользователя необходимо:

1. Открыть папку «Пользователи» в окне программы Проводник или в окне папки Secret Net.

2. Установить курсор мыши в области списка пользователей так, чтобы он не попадал ни на один из элементов списка, и нажать правую кнопку мыши.

3. В контекстном меню активизировать команду «Создать\Пользователя». В списке пользователей появится новый объект.

На имя пользователя накладываются следующие ограничения:

· имя пользователя может состоять только из латинских символов, цифр и служебных символов (символы латинской раскладки клавиатуры) и не может превышать 20 символов;

· имя пользователя не должно содержать символов `пробел';

· имя пользователя должно быть уникальным в системе;

· список пользователей компьютера может содержать не более 1020 объектов.

При создании пользователя параметры его работы будут автоматически приведены в соответствие со значениями, хранящимися в шаблоне, установленном в качестве шаблона по умолчанию.

Если в шаблоне по умолчанию установлен параметр «Запрос пароля», на экране появится диалог определения пароля пользователя:

4. Указать пароль для входа пользователя в систему.

После того как новый пользователь создан, необходимо перейти к определению параметров и режимов его работы на компьютере и, если это необходимо, включить нового пользователя в соответствующие группы пользователей.

Переименование пользователя

Для изменения имени пользователя необходимо:

1. Открыть папку «Пользователи» в окне программы Проводник или в окне папки Secret Net. На экране появится список пользователей компьютера.

2. Вызвать контекстное меню для ярлыка с именем нужного пользователя и активизировать команду «Переименовать».

3. Ввести с клавиатуры новое имя пользователя.

4. Нажать клавишу <Enter>.

Удаление пользователя

Для удаления пользователя необходимо:

1. Открыть папку «Пользователи» в окне программы Проводник или в окне папки Secret Net. На экране появится список пользователей компьютера.

2. Вызвать контекстное меню для ярлыка с именем удаляемого пользователя и активизировать команду «Удалить». Или выбрать ярлык и нажать клавишу <Delete> (или одноименную кнопку панели инструментов).

3. Подтвердить удаление в появившемся на экране окне запроса.

Запрещено удаление пользователя, являющегося администратором безопасности компьютера по умолчанию, а также пользователей с именами SUPERVISOR и NETWORK.

Предоставление привилегий

В системе Secret Net пользователю могут быть предоставлены привилегии двух типов:

1. Привилегии на работу с системой - эти привилегии разрешают пользователю превышать свои права на доступ к ресурсам компьютера и игнорировать некоторые другие ограничения его работы в системе;

2. Привилегии на администрирование системы защиты - эти привилегии разрешают пользователю управлять работой системы защиты.

Для предоставления привилегий пользователю необходимо:

1. Вызвать на экран окно управления свойствами пользователя.

2. Активизировать диалог «Привилегии»:

3. Предоставить пользователю необходимые привилегии на работу с системой (см. табл. 1 и 2). Список «Привилегии на работу с системой» содержит перечень всех привилегий этого типа. Привилегии, предоставленные пользователю в данный момент, имеют отметку слева от названия привилегии.

Привилегии на доступ к ресурсам компьютера, предоставленные пользователю, имеют высший приоритет при определении прав доступа пользователя к ресурсам.

4. Предоставить пользователю необходимые привилегии на администрирование системы защиты. Список «Привилегии на администрирование системы» содержит перечень всех привилегий на администрирование системы Secret Net, которые могут быть предоставлены пользователю. Привилегии, предоставленные пользователю, имеют отметку слева от названия привилегии.

5. Нажать кнопку «ОК».

Таблица 1

Привилегии на работу с системой

Привилегии	**Назначение**
Видимость дисков	Во всех программах, отображающих список существующих логических дисков, показывать пользователю логические диски, даже если доступ к этим дискам ему запрещен (определены права на доступ к диску «Нет доступа»)
Видимость каталогов	Во всех программах, отображающих список существующих каталогов, показывать пользователю каталоги, даже если доступ к этим каталогам ему запрещен (определены права на доступ к каталогу «Нет доступа»)
Видимость файлов	Во всех программах, отображающих список существующих файлов, показывать пользователю имена файлов, даже если доступ к этим файлам ему запрещен (определены права на доступ к файлу «Нет доступа»)
Без атрибутов на дисках	Отменить для пользователя все ограничения на доступ к логическим дискам
Без атрибутов на каталогах	Игнорировать присвоенные каталогам атрибуты доступа и владения. Пользователь наделяется правами полного доступа ко всем каталогам, находящимся на локальных дисках компьютера (если это не запрещено атрибутами доступа к дискам)
Окончание табл. 1	
Назначение	Назначение
Без атрибутов на файлах	Игнорировать атрибуты доступа и владения, присвоенные файлам. Пользователь наделяется правами полного доступа ко всем файлам, находящимся на локальных дисках компьютера (если это не запрещено

	атрибутами доступа к дискам и каталогам)
Без ограничений по настройкам	Игнорировать ограничения и запреты, установленные для пользователя: · при выключении мягкого режима работы для замкнутой программной среды и мягкого режима для атрибутов; · при настройке свойств пользователя в диалоге «Запреты»; · расписанием работы пользователя на компьютере

Шаблоны настройки свойств пользователей

Для упрощения процедуры настройки свойств пользователей удобно использовать шаблоны. Например, если требуется определить одинаковые свойства для нескольких пользователей, сохраните настройки свойств в шаблоне с заданным именем. После этого достаточно установить этот шаблон в качестве текущего для любого пользователя компьютера, и настройки свойств этого пользователя будут автоматически приведены в соответствие со значениями, хранящимися в шаблоне.

. Настройка свойств пользователя с помощью шаблона

Для настройки свойств пользователя используется один из способов:

Способ 1:

1. Вызвать на экран окно управления свойствами пользователя.

2. В группе полей «Шаблон настроек» нажать кнопку и выбрать название шаблона из открывшегося списка.

3. Нажать кнопку «ОК».

В результате выполненных операций:

· в состав папки с именем пользователя добавится ярлык-ссылка с названием шаблон настроек;

· в состав папки с названием шаблона - ярлык-ссылка с именем соответствующего пользователя;

настройки свойств пользователя будут автоматически приведены в соответствие со значениями, хранящимися в шаблоне.

Следует помнить, что после назначения пользователю шаблона настройки, контролируются изменения любого из свойств пользователя, заданного этим шаблоном. При попытке сохранения изменений система предложит выбрать вариант выполнения этой операции.

Для просмотра списка пользователей, для которых шаблон является текущим необходимо:

1. Запустить программу Проводник. Найти и открыть папку «Secret Net 9x».

2. Открыть папку «Шаблоны настроек».

3. Выбрать ярлык с названием шаблона.

На экране отобразится список ярлыков-ссылок с именами пользователей, для которых выбранный шаблон является текущим.

Создание шаблона

Для создания нового шаблона используется один из способов:

Способ 1:

1. Вызвать на экран окно управления свойствами пользователя.

2. В группе полей «Шаблон настроек» нажать кнопку «Создать». На экране появится диалог «Создание шаблона настроек»:

3. Ввести в поле «Название шаблона» название нового шаблона, а в поле «Описание» - дополнительную информацию о нем.

4. Нажать кнопку «ОК» для сохранения нового шаблона в списке шаблонов.

5. Закрыть окно управления свойствами пользователя.

Управление шаблонами настройки

Для управления шаблонами необходимо:

1. Запустить программу Проводник.

2. Найти и открыть папку «Secret Net».

Для управления шаблонами настройки свойств пользователей необходимо обладать привилегией «Просмотр и изменение (Уровень 3)» группы привилегий «Параметры работы других пользователей».

3. Вызвать на экран диалог управления шаблонами одним из следующих способов:

· активизировав в контекстном меню папки «Secret Net» команду «Шаблоны настроек»;

· активизировав в контекстном меню папки «Шаблоны настроек» команду «Свойства».

·

На экране появится диалог управления шаблонами настройки свойств пользователей:

4. Выполнить необходимые действия.

5. Нажать кнопку «ОК».

Для назначения шаблона по умолчанию используются следующие способы:

· Постановка отметки в поле переключателя, содержащего название шаблона.

· Выбор названия шаблона в списке, нажатие на кнопку «По умолчанию».

Кроме способов, изложенных выше, можно установить шаблон по умолчанию следующим образом: вызвав контекстное меню ярлыка с названием шаблона, который требуется назначить шаблоном по умолчанию, и активизировав команду «Сделать шаблоном по умолчанию».

Для переименования шаблона необходимо:

1. Выбрать название шаблона в списке.

2. Нажать кнопку «Изменить».

3. Ввести необходимую информацию в поле «Название шаблона/Описание».

4. Нажать кнопку «ОК».

Кроме способа, изложенного выше, можно изменить дополнительную информацию о шаблоне следующим образом: вызвать контекстное меню ярлыка с названием шаблона, описание которого необходимо изменить, и выбрать команду «Свойства». Изменить дополнительную информацию о шаблоне в текстовом поле группы «Общие сведения».

Для удаления шаблона необходимо:

1. Выбрать название шаблона в списке.
2. Нажать кнопку «Удалить».
3. Подтвердить удаление шаблона.

Задание 1. Изменение настроек, сохраненных в шаблоне

Для изменения настроек необходимо:

1. Запустить программу Проводник. Найти и открыть папку «Secret Net».

2. Открыть папку «Шаблоны настроек» и выбрать ярлык с названием шаблона, настройки которого требуется изменить.

Рис. 11. Диалог «Свойства шаблонов»

3. Вызвать контекстное меню ярлыка шаблона и активизировать команду «Свойства».

4. Указать необходимые значения параметров в диалоге, появившемся на экране.

5. Нажать кнопку «ОК».

Настройки свойств пользователей, для которых этот шаблон является текущим, будут изменены в соответствии с новыми значениями параметров.

Задание 2. Группы пользователей

Для управления группами пользователей необходимо раскрыть список групп одним из следующих способов:

· Запустить программу Проводник. Найти и открыть папку «Secret Net». Открыть папку «Группы пользователей».

· Выбрать в контекстном меню ярлыка Secret Net, расположенного на Рабочем столе Windows, команду «Открыть». Открыть папку «Группы пользователей».

Рис. 12. Контекстные меню для управления группами пользователей

Задание 3. Создание группы

Для создания новой группы необходимо:

1. Установить курсор мыши в области списка групп пользователей так, чтобы он не попадал ни на один из элементов списка, и нажать правую кнопку мыши.

2. В контекстном меню активизировать команду «Создать\Группу». В списке групп пользователей появится новый объект.

3. Изменить название группы, если это необходимо, руководствуясь следующими правилами:

· название группы пользователей может состоять только из латинских символов, цифр и служебных символов (символы латинской раскладки клавиатуры) и не может превышать 20 символов;

· название группы не должно содержать символов «пробел» и должно быть уникальным в системе.

Число групп ограничено и не может превышать 49.

Задание 4. Изменение свойств группы

Для изменения свойств группы необходимо:

1. Вызвать контекстное меню для ярлыка с названием нужной группы и активизировать команду «Свойства». На экране появится диалог:

Рис. 13. Диалог «Свойства группы пользователей»

2. Отредактировать текстовое поле «Заметки», которое может содержать до 255 символов справочной информации о группе пользователей. Эти сведения отображаются в колонке «Заметки» списка групп пользователей.

3. Нажать кнопку «ОК».

Задание 5. Управление составом группы

Для просмотра состава группы пользователей необходимо:

Выбрать в списке групп пользователей ярлык с названием нужной группы. На экране отобразится список ярлыков-ссылок с именами пользователей, входящих в состав данной группы.

Для просмотра списка групп, в которые включен пользователь необходимо:

1. Найти и открыть папку «Пользователи».

2. Выбрать ярлык с именем пользователя. В правой (или левой) части окна Проводника отобразится список ярлыков ссылок с названиями групп пользователей, в которые включен пользователь.

Для добавления пользователя в состав группы необходимо:

1. Открыть папку «Пользователи» в окне программы Проводник или в окне папки Secret Net.

2. Выбрать из списка пользователей ярлык с именем пользователя, которого необходимо включить в состав группы.

Можно добавить в состав группы несколько пользователей одновременно. Для выбора нескольких объектов используются клавиши <Shift> и <Ctrl>. Также можно использовать стандартную операцию DRAG-AND-DROP для копирования и вставки объектов в папку.

3. Вызвать контекстное меню для ярлыка с именем пользователя и активизировать команду «Копировать».

4. Открыть папку «Группы пользователей».

5. Вызвать контекстное меню для ярлыка нужной группы и активизировать команду «Вставить».

В результате выполненных действий в папку с именем пользователя добавится ярлык-ссылка с названием группы пользователей, а в папку с названием группы - ярлык-ссылка с именем пользователя. При этом пользователь наделяется правами доступа к ресурсам, которыми обладает данная группа.

Для исключения пользователя из состава группы необходимо:

5. Найти и выбрать ярлык группы пользователей, из которой необходимо исключить пользователя.

6. Выбрать ярлык-ссылку с именем пользователя, которого необходимо исключить из состава группы.

7. Вызвать контекстное меню для ярлыка-ссылки с именем пользователя и активизировать команду «Удалить».

В результате выполненных действий из списка пользователей, входящих в группу, удалится ярлык-ссылка с именем пользователя, а из списка групп пользователей, в которые входит данный пользователь, удалится ярлык-ссылка с именем группы.

Задание 6. Удаление группы пользователей

Для удаления группы пользователей необходимо:

1. Открыть папку «Группы пользователей» в окне программы Проводник или в окне папки Secret Net. На экране появится список групп пользователей.

2. Вызвать контекстное меню для ярлыка с названием удаляемой группы и активизировать команду «Удалить». Или выбрать ярлык и нажать клавишу <Delete>.

3. Подтвердить удаление в появившемся на экране окне запроса.

Внимание! При удалении группы пользователей удаляются все ярлыки-ссылки с именами пользователей, входивших в эту группу. Эти пользователи теряют права доступа к ресурсам файловой системы компьютера, для которых удаленная группа являлась группой владельцев ресурса.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 6

Исследование управления организационными подразделениями, делегирования полномочий

Цель работы: Ознакомиться с управлением организационными подразделениями, делегирование полномочий

Теоретическая часть:

Администрирование учетных записей групп

Мы рассмотрим группы и их реализацию в среде Windows 2000. Вы узнаете, что такое группы и как они упрощают администрирование учетных записей пользователей. Кроме того, мы обсудим типы групп и реализацию групп в домене, а также реализацию локальных и встроенных групп.

Группа (group) — это набор учетных записей пользователей. Группы упрощают администрирование, позволяя назначать разрешения и права группе пользователей, а не каждой отдельной учетной записи. Пользователи могут быть членами нескольких групп.

Назначая разрешения, Вы предоставляете пользователям доступ к определенным ресурсам и определяете права доступа. Если, например, нескольким пользователям требуется считать один файл, добавьте их учетные записи в группу. Затем дайте группе разрешение на считывание файла. Права дают возможность выполнять системные задачи, например, изменять системное время, архивировать или восстанавливать файлы, а также локально регистрироваться в системе.

Кроме пользователей, в группу можно добавлять контакты, компьютеры и другие группы. Добавляя компьютеры в группу, Вы можете упростить предоставление доступа системной задаче одного компьютера к ресурсам другого.

Реализация групп в домене

Для внедрения групп в домене надо понимать типы групп, области действия групп и правила членства в группе. Эти знания помогут Вам создавать группы, добавлять в них новых участников, изменять область действия группы и удалять их.

Типы групп

Иногда группы создаются в целях защиты, например, для назначения разрешений. В других случаях создание групп не связано с соображениями безопасности, и они используются, например, для отсылки сообщений электронной почты. Таким образом, в Windows 2000 Server два типа групп:

безопасности и распространения. Тип группы определяет порядок ее использования. Группы обоих типов размещаются в хранилище Active Directory, что позволяет их применять в любом сегменте сети.

Группы безопасности

В ОС Windows 2000 доступны только группы безопасности, используемые для назначения разрешений и предоставления доступа к ресурсам. Программы поиска в хранилище Active Directory также могут использовать группы безопасности в целях, не связанных с безопасностью, например, для одновременной отсылки сообщений электронной почты нескольким пользователям. Следовательно, группа безопасности обладает всеми возможностями группы распространения.

Группы распространения

Приложения используют группы распространения в качестве списков пользователей для осуществления функций, не связанных с системой защиты. Группы распространения следует применять лишь для выполнения операций, не связанных с безопасностью, например, для одновременной отсылки сообщений электронной почты нескольким пользователям. Назначать разрешения через группу распространения нельзя.

Область действия группы

При создании группы надо определить ее тип и область действия, которая позволяет по-разному использовать группы для назначения разрешений. Область действия также определяет, в каких сегментах сети группу можно использовать. По области действия группы делятся на локальные группы домена, глобальные и универсальные.

Локальная группа домена

Чаще всего используется для назначения разрешений доступа к ресурсам. Ее характеристики:

открытое членство — можно добавлять членов из любого домена.

доступ к ресурсам одного домена — позволяет назначать разрешения доступа к ресурсам того же домена, где была создана группа

Глобальная группа

Чаще всего применяется для организации пользователей с одинаковыми требованиями доступа к сети. Ее характеристики:

ограниченное членство — можно добавлять членов лишь из того домена, где создана группа;
доступ к ресурсам любого домена — позволяет назначать разрешения доступа к ресурсам любого домена.

Универсальная группа

Чаще всего применяется для назначения разрешений доступа к связанным ресурсам, находящимся в нескольких доменах. Ее характеристики
открытое членство — можно добавлять участников из любого домена;

доступ к ресурсам любого домена — позволяет назначать разрешения доступа к ресурсам в любом домене;
доступна лишь в доменах основного режима — в доменах смешанного режима эти группы недоступны; полный набор возможностей Windows 2000 доступен лишь в основном режиме.

Вложенность групп

Добавление одних групп в другие (вложенность групп) позволяет на порядок снизить число операций по назначению разрешений. Изучите потребности членов групп и создайте соответствующую иерархию групп. В основном режиме Windows 2000 допускает неограниченную вложенность групп. Так, можно создать группу для каждого региона, в котором имеются филиалы организации, затем добавить менеджеров из всех регионов в отдельные группы. Все региональные группы можно добавить в группу Worldwide Managers. Если региональным менеджерам потребуется доступ к некоторому ресурсу, задайте соответствующие разрешения группе Worldwide Managers. Благодаря вложенности, эта группа включает всех членов региональных групп, поэтому менеджеры из всех регионов смогут обратиться к требуемому ресурсу. Это обеспечивает упрощенное иерархичное назначение разрешений, а также децентрализованный контроль членства.

При добавлении одних групп в другие попытайтесь снизить уровень вложенности. Вложенность позволяет на порядок снизить число операций по назначению разрешений. Однако при больших уровнях вложенности контроль разрешений усложняется. Наиболее эффективен первый уровень — он позволяет снизить число операций по назначению разрешений, одновременно упрощая контроль разрешений. Кроме того, в целях контроля за назначением разрешений рекомендуется отдельно документировать состав групп. Допустим, администратор добавляет временных сотрудников в группу, созданную для разработчиков некоторого проекта. Другой администратор, не зная о временных сотрудниках, добавляет группу проекта в группу, обладающую доступом к конфиденциальной информации, и временные сотрудники получают к ней доступ, что неприемлемо.

В смешанном режиме доступен лишь один вид вложенности — глобальные группы любого домена могут входить в локальные группы доменов; в смешанном режиме универсальные группы недоступны;

В основном режиме доступны все правила членства в группах, допускаются множественные уровни вложенности.

Стратегии групп

Для эффективной работы надо определить порядок использования групп а также типы групп, которые будут задействованы в конкретных ситуациях.

Использование глобальных и локальных групп домена

Правила реализации глобальных и локальных групп домена идентичны рекомендациям по созданию стратегий групп для доменов Windows NT 3.x/4.0. Надо:

пользователей со схожими обязанностями объединить в одну группу; например, в бухгалтерии можно объединить учетные записи бухгалтеров в группу Accounting; определить, к каким ресурсам или группам ресурсов обращаются сотрудники, и создать для этого ресурса локальную группу домена; например, если в организации несколько цветных принтеров, создайте локальную группу домена Color Printers;
выявить все глобальные группы, обращающиеся к одним и тем же ресурсам, и включить эти группы в соответствующую локальную группу домена; так, можно добавить глобальные группы Accounting, Sales и Management в локальную группу домена Color Printers;
назначить локальной группе домена соответствующие разрешения; например, группе Color Printers надо назначить разрешения на доступ к цветным принтерам.

Коме того, помещая учетные записи пользователей в локальные группы домена и назначая последним разрешения, Вы не можете предоставлять разрешения вне домена. Гибкость стратегии глобальных и локальных групп домена снижается с ростом сети.

Несмотря на преимущества данной стратегии, при работе с несколькими доменами размещение учетных записей в глобальных группах и назначение им разрешений может усложнить администрирование. Если глобальным группам нескольких доменов нужны одинаковые разрешения, придется назначать их каждой группе в отдельности

Объедините пользователей со схожими обязанностями в одну группу

Создайте для совместно используемых ресурсов локальную группу домена

Добавьте в локальную группу домена глобальные группы, которым требуется доступ к ресурсам

Назначьте локальной группе домена разрешения доступа к ресурсам

Внедрение групп

Разработав план, группы можно внедрять.

Область действия следует определять в соответствии с тем, как будет использоваться группа. Так, глобальные группы рекомендуются для группировки учетных записей пользователей. Локальные доменные и универсальные группы удобны для назначения разрешений доступа к ресурсам. Глобальные группы следует включать в локальные доменные и универсальные группы.

Добавлять/удалять пользователей из универсальных групп не рекомендуется, поскольку это может сильно увеличить трафик репликации.

Перед созданием группы в домене убедитесь в наличии у Вас соответствующих прав. Члены групп Administrators и Account Operators данного домена по умолчанию обладают всеми необходимыми разрешениями. Администратор может предоставлять пользователям разрешения на создание групп в доменах или в ОП.

Имя группы должно быть интуитивным, особенно если администраторы других

доменов будут искать его в Active Directory. Если в нескольких доменах есть параллельные группы, убедитесь, что их имена также параллельны. Скажем, если в доменах имеются отдельные группы для менеджеров, система их именования должна быть согласованной, например, Managers USA и Managers Australia.

Создание групп

Для создания групп служит оснастка Active Directory Users And Computers. Их следует создавать в ОП Users или в ОП, созданных специально для групп. В процессе роста и развития организации некоторые группы могут оказаться ненужными. Такие группы надо удалять. Это поможет Вам гарантировать безопасность, т. е. Вы не присвоите разрешения доступа к ресурсам группе, которая больше не используется. Чтобы создать группу, запустите оснастку Active Directory Users And Computers. В меню Action (Действие) выберите New (Создать), а в нем команду Group (Группа). Откроется диалоговое окно New Object — Group (Новый объект — Группа), параметры которого таковы

Администрирование групп

Оснастка Active Directory Users And Computers позволяет добавлять членов в группу, изменять области действия и удалять группы.

Добавление членов в группу

В созданную группу можно добавлять членов — учетные записи пользо-вателей, контакты, другие группы и компьютеры. Компьютеры добавляются в группу для предоставления им доступа к разделяемым ресурсам других систем, например, для удаленного резервного копирования

Чтобы добавить новых членов, дважды щелкните нужную группу. В диалоговом окне свойств перейдите на вкладку Members (Члены группы) и щелкните кнопку Add (Добавить). Откроется диалоговое окно Select Users, Contacts, Or Computers (Выбор: Пользователи, Контакты и Компьютеры)

Изменение области действия групп

В процессе развития сети может возникнуть потребность в изменении области действия группы. Например, чтобы предоставить пользователям доступ к ресурсам других доменов, Вам может понадобиться преобразовать имеющуюся локальную доменную группу в глобальную. Изменить область действия группы позволяет вкладка General (Общие) диалогового окна свойств группы.

Примечание Изменять область действия группы можно лишь в доменах основного режима. В доменах смешанного режима такая операция не допускается. Кроме того, Windows 2000 не поддерживает изменение области действия универсальной группы, поскольку ограничения н членство и область действия других групп более строги.

Удаление групп

Каждая группа обладает уникальным идентификатором безопасности, SID, повторно задействовать который невозможно. SID в Windows 2000 служит для идентификации групп и присвоенных ей разрешений. Windows 2000 не использует повторно идентификаторы удаленных групп, даже если Вы

создадите группу с именем, аналогичным имени удаленной группы. Следовательно, восстановить доступ к ресурсам, воссоздав группу, нельзя.

При удалении группы удаляется лишь сама группа и связанные с ней разрешения. Учетные записи пользователей — членов группы не затрагиваются. Удаляемую группу щелкните правой кнопкой и выберите в контекстном меню команду Delete (Удалить).

Внедрение локальных групп

Локальная группа может включать учетные записи компьютера, на котором она находится. Ее рекомендуется применять для назначения разрешений доступа к ресурсам, расположенным на том же компьютере, что и группа. Windows 2000 создает локальные группы в локальной БД системы защиты. Локальные группы бывают доменными и изолированными.

Создание локальных групп

Изолированные локальные группы позволяет создать оснастка Computer Management. Локальные группы создаются в папке Groups (Группы). Чтобы создать локальную группу, раскройте в дереве консоли папку Local Users And Groups (Локальные пользователи и группы) и щелкните подпапку Groups (Группы). Затем в меню Action выберите команду New Group (Создать группу). В открывшемся диалоговом окне введите имя и описание группы. Параметры диалогового окна New Group (Создание группы) описаны ниж

Встроенные группы

В Windows 2000 четыре типа встроенных групп: глобальные, доменные локальные, изолированные локальные и системные. Встроенные группы обладают предопределенным набором членов и прав. Windows 2000 автоматически создает такие группы, чтобы Вам не приходилось вручную создавать группы и назначать разрешения для часто используемых функций.

Встроенные глобальные группы

Позволяют объединять учетные записи общего типа. Windows 2000 по умолчанию добавляет членов в некоторые встроенные глобальные группы. Вы также можете добавлять в них новых членов, чтобы предоставить им права и разрешения группы.

При создании домена Windows 2000 создает встроенные глобальные группы в хранилище Active Directory. Чтобы присвоить встроенной глобальной группе права, ее можно добавить в локальную группу домена или явно назначить ей нужные права и разрешения.

ОП Users содержит все встроенные группы домена. Ниже перечислены стандартные участники наиболее распространенных встроенных глобальных групп:

Встроенная локальная группа домена

Windows 2000 создает встроенные локальные группы домена, чтобы предоставить пользователям права и разрешения на выполнение задач в хранилище Active Directory, а также на контроллерах домена Встроенная

локальная группа в целом работает аналогично локальной группе домена, единственное отличие в том, что ее нельзя удалить.
Встроенные локальные группы домена предоставляют добавляемым в них учетным записям пользователей и глобальным группам набор предопределенных прав и разрешений. Наиболее распространенные встроенные локальные группы, а также привилегии, которыми обладают их члены, таковы:

Локальная группа	Описание
Account Operators (Операторы учета)	Создавать, удалять и изменять права групп и учетных записей пользователей. Члены группы не имеют разрешения на изменение группы Administrators и любых групп операторов.
Server Operators (Операторы сервера)	Предоставлять в совместное использование дисковые ресурсы, архивировать и восстанавливать файлы на контроллере домена.
Print Operators (Операторы печати)	Настраивать и управлять сетевыми принтерами на контроллерах домена.
Administrators (Администраторы)	Выполнять все административные задачи на любых контроллерах домена, включая сам домен. По умолчанию членами данной локальной группы являются учетная запись Administrator, глобальные группы Domain Admins и Enterprise Admins.
Backup Operators (операторы архива)	Архивировать и восстанавливать все контроллеры домена при помощи утилиты Windows Backup (Архивация).
Qests (Гости)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются учетная запись Guest и глобальная группа Domain Guests. При установке некоторые службы автоматически добавляют пользователей в эту локальную группу. Например, службы Microsoft Internet Information Services (IIS) автоматически добавляют во встроенную группу Guests учетные записи анонимных пользователей.
Users (Пользователи)	Обращаться лишь к тем ресурсам и выполнять лишь те задачи, на которые у них имеются разрешения. Члены группы не могут вносить постоянные изменения в конфигурацию рабочего стола. По умолчанию членами этой группы являются группа Domain Users, специальные группы Authenticated Users (Прошедшие проверку) и INTERACTIVE (Интерактивные). Поддержка системных групп осуществляется Windows 2000; удалить их нельзя. Группу Users рекомендуется применять для предоставления всем учетным записям домена прав и разрешений,

	которыми должен обладать каждый пользователь.

Встроенные локальные группы

На всех изолированных и рядовых серверах и компьютерах с Windows 2000 Professional есть встроенные локальные группы. Они предоставляют разрешения на выполнение задач (восстановление и архивирование файлов, изменение системного времени, администрирование ресурсов системы и др.) на отдельном компьютере. Windows 2000 помещает встроенные локальные группы в папку Groups (Группы) оснастки Computer Management. Как и встроенные доменные локальные, удалить встроенные недоменные локальные группы нельзя.

Права, которыми обладают члены встроенных локальных групп, таковы:

Встроенные системные группы

На всех Windows 2000-компьютерах есть встроенные системные группы (в Windows NT — специальные группы). Системные группы не имеют определенного списка членов, который можно было бы изменять; в разное время состав членов таких групп может различаться в зависимости от метода доступа пользователя к ресурсу или компьютеру. При администрировании системные группы недоступны, однако они отображаются при назначении прав и разрешений доступа к ресурсам.

Состав системных групп в Windows 2000 основан на способе доступа к компьютеру, а не на том, какие пользователи работают с компьютером. Наиболее распространены встроенные системные группы:

Задание 1: создание групп

Вы создадите глобальную группу защиты и добавите в нее членов — две ранее созданные учетные записи Jane Doe и John Smith. Затем Вы создадите локальную группу домена и назначите ей разрешения доступа к отчетам о продажах. После этого Вы предоставите членам глобальной группы защиты доступ к отчетам о продажах, добавив эту группу в локальную группу домена.

Задание 2: создайте глобальную группу, добавьте участников и организуйте учетные записи пользователей

Создайте глобальную группу защиты, добавьте в нее членов и переместите пользователя из одного организационного подразделения (ОП) в другое.

1. Убедитесь, что оснастка Active Directory Users And Computers открыта и в фокусе
2. В дереве консоли щелкните узел ОП Sales. На правой панели появится учетная запись пользователя Jane Doe.
3. В меню Action выберите New (Создать), а затем — команду Group. Откроется диалоговое окно New Object — Group (Новый объект — Группа).

4. Убедитесь, что выбраны переключатели Global (Глобальная) и Security (Группа безопасности)

5. В поле Group Name (Имя группы) введите **Sales** и щелкните ОК. На правой панели узла появится новая группа.

6. На правой панели дважды щелкните группу Sales. Откроется диалоговое окно Sales Properties (Свойства: Sales).

7. Перейдите на вкладку Members (Члены группы).

8. Щелкните кнопку Add (Добавить). Откроется диалоговое окно Select Users, Contacts, Computers, Or Groups (Выбор: Пользователи, Компьютеры, Контакты или Группы); в списке Look In (Искать в) будет выбрано study.bmstu.

9. В списке учетных записей, групп и компьютеров щелкните Jane_Doe и, удерживая клавишу Ctrl, щелкните John_Smith. Будут выбраны обе учетные записи. Учетная запись Jane Doe находится в ОП study.bmstu /Sales, a John Smith — в ОП study.bmstu / Users.

10. Щелкните кнопку Add (Добавить). Учетные записи Jane Doe и John Smith стали членами глобальной группы защиты Sales.

11. Щелкните кнопку ОК.

12. Снова щелкните кнопку ОК, чтобы закрыть диалоговое окно Sales Properties (Свойства: Sales). В организационных целях Вы решили переместить учетную запись John Smith в ОП Sales.

13. Щелкните ОП Users.

14. На правой панели щелкните учетную запись John Smith.

15. В меню Action (Действие) выберите команду Move (Переместите) Откроется одноименное окно.

16. Выберите ОП Sales и щелкните кнопку ОК. Учетная запись John Smith больше не отображается в правой панели ОП Users.

17. В дереве консоли щелкните ОП Sales. В правой панели отображены учетные записи John Smith и Jane Doe и глобальная группа безопасности Sales.

18. Дважды щелкните глобальную группу Sales. Откроется диалоговое окно Sales Properties (Свойства: Sales).

19. Перейдите на вкладку Members (Члены группы). Учетная запись John Smith по-прежнему член группы Sales, но находится теперь в папке study.bmstu /Sales.

20. Щелкните кнопку ОК.

Задание 3: создайте и используйте локальную группу домена
Создайте локальную группу домена для предоставления доступа к отчетам о продажах. В нее Вы добавите глобальную группу безопасности, созданную на этапе 1.

1. Щелкните правую панель консоли, чтобы снять выделение с группы Sales.

2. В меню Action выберите New, а затем — команду Group. Откроется диалоговое окно New Object — Group.

3. В поле Group Name (Имя группы) введите **Reports.**

4. Щелкните переключатели Security (Группа безопасности) и Domain Local (Локальная в домене).

5. Щелкните кнопку ОК. На правой панели для ОП Sales появится локальная группа домена.

6. На правой панели дважды щелкните группу Reports. Откроется диалоговое окно Reports Properties (Свойства: Reports)

7. Перейдите на вкладку Members (Члены группы).

8. Щелкните кнопку Add (Добавить). Откроется диалоговое окно Select Users, Contacts, Computers, Groups.

9. В списке Look In (Искать в) выберите пункт Entire Directory (Вся папка).

Будут отображены учетные записи и группы всех доменов, а также расположение этих учетных записей и групп.

10. В списке учетных записей, групп и компьютеров щелкните заголовок Name (Имя).

Поле Name (Имя) будет отсортировано по алфавиту в убывающем порядке.

11. Снова щелкните этот заголовок, чтобы отсортировать поле по алфавиту в возрастающем порядке.

12. В списке учетных записей, групп и компьютеров выделите глобальную группу Sales и щелкните кнопку Add (Добавить). Щелкните кнопку ОК. Группа Sales стала членом доменной локальной группы Reports.

13. Щелкните кнопку ОК.

14. Закройте оснастку Active Directory Users And Computers.

Задание 4: назначьте разрешения NTFS

Вы назначите локальной группе домена Reports разрешения NTFS и проверите доступ к папке sales. Выполняйте упражнение на контроллере домена (по сети).

1. Создайте на диске С: папку с именем Dept.

2. Сделайте эту папку общей с именем ресурса Dept, а в поле Comment (Комментарий) введите **Department share.**

Для общего ресурса задавать разрешений не надо, так как папка Dept создана на томе NTFS.

3. Создайте в папке Dept подкаталог Sales.

4. Выделите папку Sales.

5. В меню File (Файл) выберите команду Properties (Свойства). Откроется диалоговое окно Sales Properties (Свойства: Sales).

6. Перейдите на вкладку Security (Безопасность). Системной группе Everyone (Все) предоставлены полные права управления данной папкой.

7. Снимите флажок Allows Inheritable Permissions From Parent To Propagate To This Object (Переносить наследуемые от родительского объекта разрешения на этот объект). Появится сообщение Security (Безопасность) с описанием доступных вариантов выбора.

8. Щелкните кнопку Remove (Удалить).
Откроется диалоговое окно Sales Properties (Свойства: Sales).

9. Щелкните кнопку Add (Добавить).
Откроется диалоговое окно Select Users, Computers, Or Group.

10. В списке Look In (Искать в) выберите пункт Entire Directory (Вся папка).

11. В списке учетных записей, групп и компьютеров выделите Reports и щелкните кнопку Add.

12. Щелкните кнопку OK.
В диалоговом окне свойств папки Sales показывается, что локальной группе Reports предоставлены разрешения Read & Execute (Чтение и выполнение), List Folder Contents (Просмотр содержимого папки) и Read (Чтение).

13. Пометьте флажок Write (Запись) и щелкните кнопку OK.

14. Закройте окно Dept и завершите сеанс Administrator (Администратор).

15. Зарегистрируйтесь в системе как Jane_Doe с паролем student и откройте в окне My Computer (Мой компьютер) папку C:\Dept\Sales.

16. В меню File выберите New, а затем — Text Document (Текстовый документ).
В окне Sales появится файл New Text Document (Новый текстовый документ).

17. Дважды щелкните этот файл.
Откроется окно программы Notepad (Блокнот).

18. Введите несколько символов и закройте Notepad.
Появится запрос на сохранении изменений.

19. Щелкните кнопку Yes (Да).

20. Закройте окно Sales.

21. Завершите сеанс Jane_Doe и зарегистрируйтесь как Bob_Train без пароля.
В случае ошибки убедитесь, что Вы пытаетесь зарегистрироваться в интервал времени, когда пользователю Bob Train разрешено работать в системе. Вы задали этот интервал в одном из предыдущих упражнений данной главы.

22. Попробуйте обратиться к папке C:\Dept\Sales.
Сообщение Dept известит об отказе в доступе.
Дело в том, что Bob Train — не член глобальной группы Sales, которая в свою очередь включена в доменную локальную группу Report. Доступ к локальным папкам тоже невозможен, так как разрешения NTFS распространяются и на сетевой, и на локальный доступ.

23. Щелкните кнопку OK и закройте окно Dept.

24. Завершите сеанс Bob Train.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 7

Исследование групповой политики

Цель работы: Изучить разработку групповой политики

Теоретическая часть:

Групповые политики – средства централизованного управления настройками компьютеров пользователей. Они могут применяться для управления параметрами рабочего стола пользователя и различных приложений, набором разрешенных приложений, системными привилегиями, параметрами системы безопасности, автоматической установкой программного обеспечения и т.д.

Обычно групповые политики используются для управления настройками компьютеров в домене, однако существует возможность работы с локальной политикой компьютера, что позволяет использовать часть возможностей групповых политик при администрировании отдельного компьютера.

Концепции групповой политики

Групповые политики представляют собой набор параметров конфигурации компьютеров и окружения пользователя, хранящиеся в виде отдельных объектов. Политики применяются к компьютеру и пользователю во время загрузки компьютера и входа пользователя в систему соответственно. Каждый параметр политики вызывает определенные изменения в системном реестре Windows, таким образом, любое изменение, которое вы осуществляете на компьютере при помощи групповых политик, вы можете осуществить при помощи редактора реестра. Однако групповые политики предоставляют гораздо более гибкие и удобные средства для управления, снижая тем самым издержки на настройку компьютеров пользователей. Одним из самых больших преимуществ групповых политик является централизованное применение определенных настроек для всех (или части) компьютеров или пользователей в домене.

Объекты групповой политики

Для определения параметров конфигурации для некоторой группы пользователей и/или компьютеров создаются объекты групповой политики (Group Policy Objects, GPO) – законченные наборы параметров политики. Каждый объект групповой политики хранится в каталоге Active Directory в контейнере групповой политики (Group Policy Container, GPC). Кроме того, объекты группой политики хранятся в виде структуры папок, называемой шаблоном групповой политики (Group Policy Template, GPT). Обычно в GPC хранятся редко изменяемые и небольшие по размеру параметры, а в GPT хранятся часто изменяемые параметры и большие массивы данных. Внутренняя структура контейнеров и шаблонов групповой политики скрыта от всех пользователей системы, даже от администратора.

Объекты групповой политики могут применяться на следующих уровнях иерархии домена Windows Server 2008 R2:

сайт;

домен;

организационное подразделение.

Несколько контейнеров Active Directory могут быть связаны с одним объектом групповой политики. В свою очередь, один контейнер Active Directory может быть связан с несколькими объектами групповой политики. Таким образом, на компьютер в домене может распространяться действие неограниченного числа доменных объектов групповой политики, хранящихся в Active Directory.

Локальные объекты групповой политики

На каждом компьютере Windows имеется локальный объект групповой политики, который присутствует независимо от того, является ли компьютер членом домена и есть ли сведения о нем в Active Directory. Однако параметры доменных объектов групповой политики могут перекрывать параметры локальных объектов, поэтому при работе компьютера в домене параметры локального объекта групповой политики меньше всего влияют на конфигурацию окружения пользователя.

По умолчанию в локальном объекте групповой политики определены только параметры безопасности.

Локальный объект групповой политики хранится в папке %systemroot%\system32\GroupPolicy. Все аутентифицированные пользователи компьютера имеют право на чтение и применение локальной политики, однако право ее изменения имеют только члены группы Администраторы.

Контейнеры групповой политики

Контейнер групповой политики (GPC) является объектом каталога Active Directory, хранящим свойства объекта групповой политики. Для каждого параметра групповой политики хранится номер версии, позволяющий отслеживать и синхронизировать изменения как между GPC и GPT, так и между различными контроллерами домена и серверами глобального каталога. Также GPC хранит информацию об активности объекта групповой политики.

Также GPC содержит данные хранилища классов Windows Server 2003, используемого для централизованного развертывания приложений на компьютерах домена.

Контейнер групповой политики (также, как и GPT), содержит два основных подконтейнера, хранящих параметры групповой политики:

Конфигурация компьютера – в этом контейнере собраны все параметры, действующие на всех пользователей компьютера. Параметры применяются только к объектам компьютеров, находящихся в контейнере с настроенной групповой политикой.

Конфигурация пользователя – в этом контейнере собраны параметры, действующие только на отдельного пользователя компьютера. Параметры

применяются только к объектам учетных записей пользователей, находящихся в контейнере с настроенной групповой политикой.

Создание и применение групповых политик

Для создания объектов групповой политики, привязки к контейнерам Active Directory используется консоль Управление групповой политики. Для запуска консоли Управление групповой политики необходимо выполнить следующую последовательность действий:

Выполните вход в операционную систему под управлением Windows Server 2008 R2 под учетной записью Administrator.

Нажмите кнопку Пуск и выберите последовательно Администрирование и Управление групповой политики.

В окне Управление групповой политикой раскройте последовательно узлы Лес: school.local, Домены, school.local и выберите узел Объекты групповой политики.

Обратите внимание на два объекта групповой политики, существующих по умолчанию: Default Domain Controllers Policy и Default Domain Policy. Первый из них применятся ко всем контроллерам доменов, второй – ко всем компьютерам и пользователям, находящимся в соответствующем домене. Изменим параметры групповой политики Default Domain Policy, отключив использование только сложных паролей в домене. Для этого:

Щелкните правой кнопкой мыши по объекту групповой политики Default Domain Policy и в появившемся меню выполните команду Изменить.

В окне Редактор управления групповыми политиками раскройте последовательно узлы: Конфигурация компьютера, Политики, Конфигурация Windows, Параметры безопасности, Политика учетных записей и выберите папку Политика паролей.

Примечание. Обратите внимание на существующие параметры, которым должен удовлетворять пароль пользователя. Отключим использование сложного пароля:

В правой части окна в списке политик выберите политику «Пароль должен отвечать требованиям сложности» и в меню Действие выполните команду Свойства.

В окне Свойства: Пароль должен отвечать требованиям сложности установите переключатель в положение Отключен и нажмите кнопку OK.

Закройте окно Редактор управления групповыми политиками.

Для обновления политик требуется определенное время: от 15 мин. До нескольких часов. Чтобы форсировать обновления параметров политики необходимо:

В командной строке выполнить команду gpupdate /force.

Убедитесь, что обновление групповых политик произошло успешно и измените пароль пользователя petrovpp на простой пароль, например, 11111111.

Согласно рекомендациям компании Microsoft не рекомендуется изменять объекты групповых политик, созданных по умолчанию (Default Domain Controllers Policy и Default Domain Policy), а создавать новые объекты, давая им значимые названия (например, Параметры рабочего стола пользователя). Создадим новый объект групповой политики и настроим политику «Не отображать последнее имя пользователя»:

Откройте окно Управление групповой политикой.

В окне Управление групповой политикой раскройте последовательно узлы Лес: school.local, Домены, school.local и выберите узел Объекты групповой политики.

В окне Управление групповой политикой в меню Действие выполните команду Создать.

В окне Новый объект групповой политики в строке Имя введите имя нового объекта групповой политики, например, Не отображать последнее имя пользователя и нажмите кнопку OK.

Щелкните правой кнопкой мыши по объекту групповой политики Не отображать последнее имя пользователя и в появившемся меню выполните команду Изменить.

В окне Редактор управления групповыми политиками раскройте последовательно узлы: Конфигурация компьютера, Политики, Конфигурация Windows, Параметры безопасности, Локальные политики и выберите папку Параметры безопасности.

Примечание. Обратите внимание, что значение всех политик находится в состояние Не определено, то есть в объекте групповой политики не указано значение параметра.

В правой части окна в списке политик выберите политику «Интерактивный вход в систему: не отображать последнее имя пользователя» и в меню Действие выполните команду Свойства.

В окне Свойства: Интерактивный вход в систему: не отображать последнее имя пользователя пометьте флажок Определить следующий параметр политики, установите переключатель в положение Включен и нажмите кнопку OK.

Закройте окно Редактор объектов групповой политики.

Следующим шагом является привязка объекта групповой политики к домену school.local:

В левой части окна Управление групповой политикой щелкните правой кнопкой мыши по имени домена (school.local) и в появившемся меню выполните команду Связать существующий объект групповой политики.

В окне Выбор объекта групповой политики в списке Объекты групповой политики выберите строку с именем созданного ранее объекта

групповой политики (Не отображать последнее имя пользователя) и нажмите кнопку OK.

Примечание. Обратите внимание, что в списке Связанные объекты групповой политики появился новый объект Не отображать последнее имя пользователя.

Выполните форсированное обновление параметров групповой политики.

Перезагрузите виртуальный компьютер под управление операционной системы Windows 7 и обратите внимание, что для входа в систему необходимо указать имя пользователя и пароль (да этого момента имя пользователя указывать не надо было, оно сохранялось с последнего сеанса пользователя).

Организационные единицы

До сих пор мы настраивали политики, которые применяются для всех пользователей и компьютеров в домене. Иногда возникают настраивать различные значения одного и того же параметра для различных пользователей (например, настроить различные домашние страницы в браузере для учеников 10 и 11 классов). Для решения поставленной задачи необходимо использовать организационные единицы. Организационные единицы (OU), или подразделения, могут содержать пользователей, группы, компьютеры, принтеры и общие папки, а также другие OU. OU — это минимальная «единица» администрирования, права управления которой можно делегировать некоторому пользователю или группе. С помощью OU можно обеспечить локальное администрирование пользователей (создание, модификация и удаление учетных записей) или ресурсов.

Примечание. Организационные единицы и подразделения – это термины-синонимы; мы будем чаще использовать понятие организационная единица, говоря о структуре каталога Active Directory и его дереве, и подразделение – когда речь идет об администрировании Active Directory, делегировании управления и т. п.

В каталоге Active Directory организационные единицы представляют собой объекты типа «контейнер» и отображаются в окне оснастки Active Directory – пользователи и компьютеры как папки. Их основное назначение – группирование объектов каталога с целью передачи административных функций отдельным пользователям.

Дерево OU может отображать реальную структуру организации – административную, функциональную и т. п. При этом учитываются иерархия полномочий ответственных работников и необходимые функции управления.

Организационная единица – минимальная структурная единица, которой можно назначить собственную групповую политику. Однако OU не является структурным элементом безопасности (т. е. нельзя назначить подразделению некоторые права доступа к определенному объекту), а служит только для группирования объектов каталога. Для назначения полномочий и разрешений доступа к ресурсам следует применять группы безопасности

(security groups). Для создания организационной единицы необходимо выполнить следующую последовательность действий:

Открыть окно Active Directory – пользователи и компьютеры.

В окне Active Directory – пользователи и компьютеры выбрать узел с именем домена (school.local), в меню Действия выбрать последовательно Создать и Подразделение.

В окне Новый объект – Подразделения в строке Имя: укажите имя создаваемого подразделения, например, 10-й класс и нажмите кнопку OK.

Обратите внимание, что в структуре каталогов Active Directory появился новый элемент 10-й класс.

Раньше отмечалось, что в подразделениях могут храниться пользователи, группы, компьютеры, принтеры и общие папки, а также другие организационные единицы. В организационных подразделениях можно создавать новые элементы (пользователей и т.д.), а также переносить существующие элементы (пользователи и т.д.) из других организационных единиц. Перенесем пользователя ivanovii из папки Users в организационную единицу 10-й класс:

В окне Active Directory – пользователи и компьютеры выберите папку Users, в правой части окна выберите учетную запись Иван Иванович Иванов, в меню Действие выполните команду Вырезать.

В окне Active Directory – пользователи и компьютеры выберите организационную единицу 10-й класс и в меню Действие выполните команду Вставить, в окне Доменные службы Active Directory нажмите кнопку Да.

Обратите внимание, что в организационной единице 10-й класс появился пользователь Иван Иванович Иванов.

Создадим новый объект групповой политики, настроим параметр «Домашняя папка обозревателя» и привяжем созданную политику к организационной единице 10-й класс:

Откройте окно Управление групповой политикой.

В окне Управление групповой политикой раскройте последовательно узлы Лес: school.local, Домены, school.local и выберите узел Объекты групповой политики.

В окне Управление групповой политикой в меню Действие выполните команду Создать.

В окне Новый объект групповой политики в строке Имя введите имя нового объекта групповой политики, например, Домашняя страница и нажмите кнопку OK.

Щелкните правой кнопкой мыши по объекту групповой политики Домашняя страница и в появившемся меню выполните команду Изменить.

В окне Редактор управления групповыми политиками раскройте последовательно узлы: Конфигурация пользователя, Политики, Конфигурация Windows, Настройка Internet Explorer и выберите папку URL-адреса.

В правой части окна Редактор управления групповыми политиками дважды щелкните по параметру Важные URL-адреса.

В окне Важные URL-адреса пометьте флажок Изменить адрес домашней страницы, в строке URL-адрес домашней страницы введите http://school-collection.edu.ru и нажмите кнопку OK.

Примечание. http://school-collection.edu.ru – бесплатная коллекция цифровых образовательных ресурсов, которые помогут ученикам 10-го класса в освоение материала школьных предметов.

Закройте окно Редактор управления групповыми политиками.

В левой части окна Управление групповой политикой щелкните правой кнопкой мыши по имени организационной единицы 10-й класс и в появившемся меню выполните команду Связать существующий объект групповой политики.

В окне Выбор объекта групповой политики в списке Объекты групповой политики выберите строку с именем созданного ранее объекта групповой политики (Домашняя страница) и нажмите кнопку OK.

Выполните форсированное обновление параметров групповой политики.

Перезагрузите виртуальный компьютер под управление операционной системы Windows 7 и выполните вход в систему под учетной записью ivanovii, запустите обозреватель Internet Explorer. Какая страница загружается по умолчанию?

Результирующая политика

Для проверки параметров групповой политики на клиентском компьютере используется оснастка Результирующая политика. Для запуска оснастки Результирующая политика необходимо:

Войти в систему под управлением операционной Windows 7, воспользовавшись любой доменной учетной записью.

Нажать кнопку Пуск, в строке Найти программы и файлы ввести mmc и нажать клавишу Enter.

Примечание. mmc – Microsoft Management Console.

В окне Консоль1 – [Корень консоли] в меню Файл выполните команду Добавить или удалить оснастку.

В окне Добавление или удаление оснастки в списке Доступные оснастки выберите Результирующая политика, нажмите кнопку Добавить, а затем кнопку OK.

В окне Консоль1 – [Корень консоли] выберите папку Результирующая политика, затем в меню Действие выполните команду Создать данные RSoP.

В окне Мастер результирующей политики нажмите кнопку Далее.

В окне Выбор режима нажмите кнопку Далее.

В окне Выбор компьютера нажмите кнопку Далее.

В окне Выбор пользователя нажмите кнопку Далее.

В окне Сводка выбранных данных ознакомьтесь со списком выбранных параметров и нажмите кнопку Далее.

В окне Ошибка групповой политики ознакомьтесь с текстом ошибки и нажмите кнопку Закрыть.

В окне Завершение мастера результирующей политики нажмите кнопку Готово.

В окне Консоль 1 ознакомьтесь с параметрами групповой политики, применяемой для текущего пользователя.

Самостоятельно

Создать организационную единицу 11-й класс, поместить в нее пользователя petrovpp, создать объект групповой политики, задающий адрес домашней страницы http://ege.edu.ru (официальный сайт единого государственного экзамена), привязать созданный объект групповой политики к организационной единице 11-й класс.

Найти параметры групповой политики, отвечающие за настройки рабочего стола пользователя и на их основании создать объект групповой политики, применив к любой организационной единице.

Дополнительный материал

Задание 1. Создайте документы, описывающие политику информационной безопасности для школы, и сохраните их в личной папке.

- правила административного обслуживания;
- перечень прав и обязанностей пользователей;
- правила для администраторов;
- правила создания «гостевых» учетных записей.

Задание 2. Создание и редактирование групповой политики.

1. Откройте диалоговое окно оснастки **Пользователи и компьютеры (*Пуск/Администрирование/Active Direcory – Пользователи и компьютеры*)**.

2. Выполните редактирование политики безопасности домена, созданную автоматически:

- откройте диалоговое окно свойств домена **example.edu.ru (контекстное меню/Свойства);**
- перейдите на вкладку **Групповая политика;**

В списке будет расположена политика домена по умолчанию Default Domain Policy.

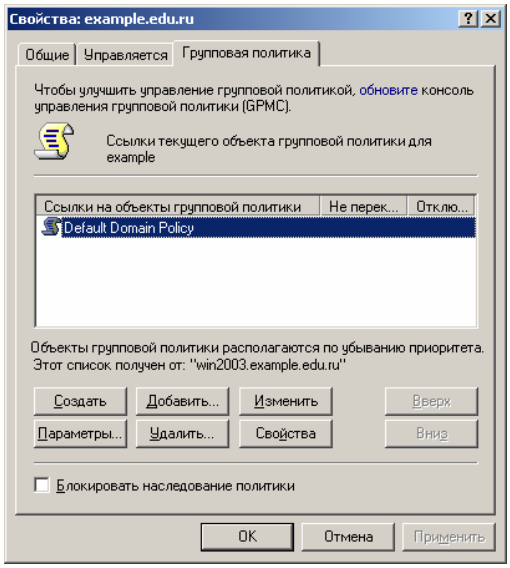


Рисунок 2. Свойства домена.

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики **Default Domain Policy** (двойной щелчок по политике);

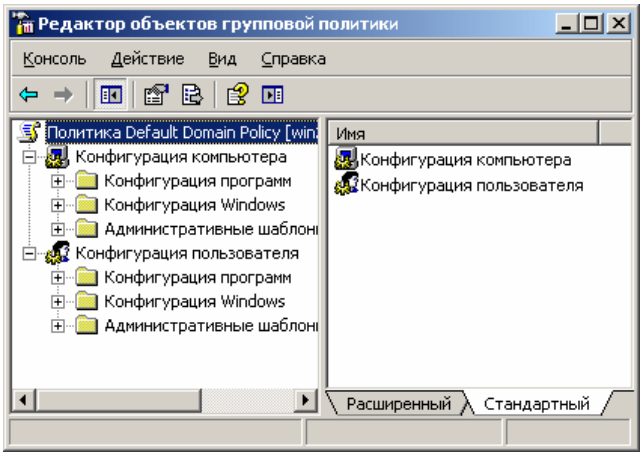


Рисунок 3. Редактор объектов групповой политики**.**

- внесите в изменения в политику паролей:
  - перейдите в раздел **Политика паролей (*Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/Политики паролей*)**;

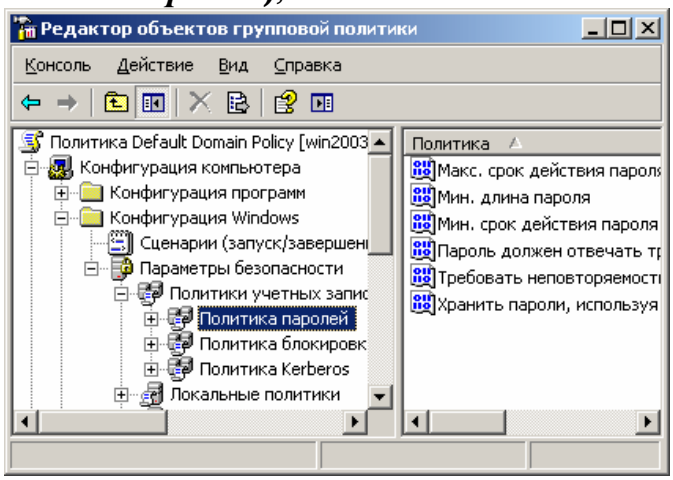


Рисунок 4. Политика паролей.

- установите **минимальную длину пароля**: откройте окно изменения параметров пароля (двойной щелчок по надписи **Мин. длинна пароля**) и введите в поле **Длина пароля не менее** – *5 (**ОК**)*;
- отключите **соответствие пароля требованиям сложности**:
- откройте диалоговое окно свойств требования сложности (двойной щелок по надписи **Пароль должен отвечать требованиям сложности**);
- установите радиокнопку *Отключить*;
- подтвердите изменения кнопкой ***ОК***;
- отключите **возможность использования экранных заставок**:
- перейдите в раздел **Экран (*Конфигурация пользователя/Административные шаблоны/Экран*)**;
- откройте диалоговое окно свойств **Использовать экранные заставки** и выберите *Отключен*;
- подтвердите изменения кнопкой ***ОК***.

- закройте **Редактор объектов групповой политики (*Консоль/Выход*)**;
- закройте диалоговое окно свойств домена кнопкой ***ОК***.

3. Создайте новую политику для учителей:

- откройте диалоговое окно свойств домена **example.edu.ru (*контекстное меню/Свойства*)** и перейдите на вкладку **Групповая политика**;
- активизируйте создание новой политики кнопкой ***Создать***;
- введите название политики - *Teachers*;
- самостоятельно измените созданную политику, отключив пользователям возможность менять фон рабочего стола.

4. Закройте редактор объектов групповой политики.

Задание 3. Создание групп и учетных записей пользователей.

1. Откройте оснастку **Пользователи и компьютеры**.
2. Создайте новую учетную запись пользователя в контейнере **Students**:

- откройте диалоговое окно **Новый объект – Пользователь**, кнопкой ***Создание нового пользователя в текущем контейнере*** ;
- введите данные о пользователе:
  - **Полное имя пользователя** – *Просто Пользователь*;
  - **Имя входа пользователя (логин)** – *JustUser*;
  - Подтвердите введенные данные кнопкой ***Далее***.

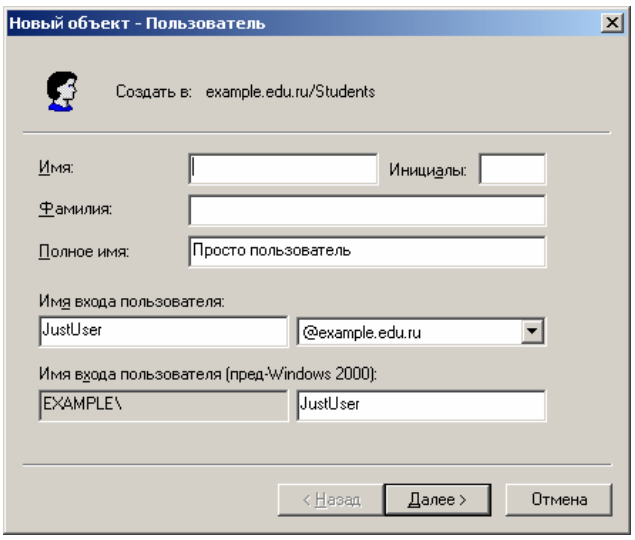


Рисунок 5. Ввод данных нового пользователя.

- установите пароль для пользователя:
  - введите в поле **Пароль** – *User1234*;
  - введите в поле **Подтверждение** – *User1234*;
  - установите флажок *Срок действия пароля не ограничен*;
  - завершите ввод пароля кнопкой ***Далее***.

В правой области отобразиться запись, соответствующая созданному пользователю.

3. Введите более полную информацию о пользователе:

- откройте диалоговое окно свойств пользователя (двойной щелчок по надписи **Просто пользователь**);
- введите в поле **Описание** – *это тестовый пользователь*;
- введите в поле **Комната** - номер кабинета в котором проходит занятие - *316*;
- введите в поле **Телефон** – <номер своего мобильного телефона>;
- укажите адресные данные на вкладке **Адрес**;
- укажите несколько дополнительных телефонов пользователя на вкладке **Телефоны**;
- завершите изменение данных пользователя кнопкой ***ОК***.

4. Создайте группу **group1** в контейнере **Students**:

- откройте диалоговое окно создания групп (***контекстное меню/Создать/Группа***);
- введите **имя группы – *group1*;**
- **завершите создание группы кнопкой *ОК*.**

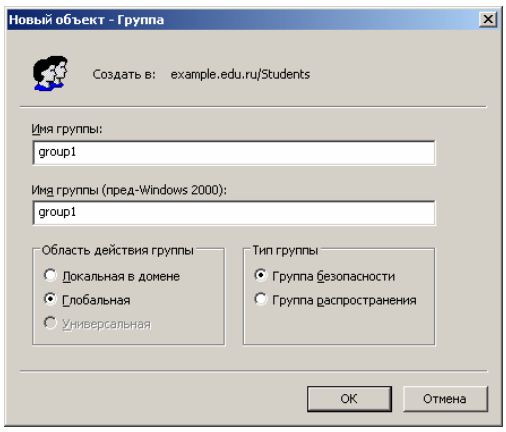


Рисунок 6. Создание группы.

5. Задайте дополнительную информацию для группы group1:

- откройте диалоговое окно свойств группы (*двойной щелчок по надписи group1*);
- введите в поле Описание – *Это тестовая группа*;
- завершите изменение данных группы кнопкой *ОК*.

6. Включите созданного ранее пользователя *Просто пользователь (JustUser)* в группу group1:

- откройте диалоговое окно свойств пользователя (*двойной щелчок по записи пользователя*);
- перейдите на вкладку Член групп;
- откройте диалоговое окно выбора группы кнопкой *Добавить*;
- введите название группы – *group1*;
- завершите добавления пользователя в группу кнопкой *ОК*.
- закройте диалоговое окно свойств пользователя кнопкой *ОК*.

7. Выполните выход из системы с повторным входом для активации изменений в политике безопасности.

Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.

8.

9. Измените пароль созданного ранее пользователя:

- активизируйте раздел Students;
- задайте новый, более простой пароль пользователю Просто пользователь:
  - откройте диалоговое окно задания пароль (*контекстное меню/Смена пароля*);
  - введите в поле Пароль – *123*;
  - введите в пол Подтверждение пароля – *123*;

Обратите внимание что сообщений по слишком простом пароле не было.

-

10. Исключите созданного ранее пользователя из группы group1:

- откройте диалоговое окно свойств группы;
- перейдите на вкладку Члены группы;

- выделите в списке удаляемого пользователя и щелкните по кнопке *Удалить*;
- подтвердите удаление кнопкой *Да*;
- закройте диалоговое окно свойств группы кнопкой *ОК*.

11. Включите созданного ранее пользователя в администраторы домена:
    - откройте диалоговое окно свойств пользователя Просто пользователь;
    - перейдите на вкладку Член групп и щелкните *Добавить*;
    - введите в поле *Администраторы домена*;
    - завершите добавление в группу кнопкой *ОК*;
    - закройте окно свойств пользователя кнопкой *ОК*.
12. Закройте оснастку Пользователи и компьютеры.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод.

Лабораторная работа № 8

Управление службой резервного копирования

Тема: Создание резервных копий.
Цель: научиться выполнять архивирование данных и пользоваться службой восстановления системы.

Теоретические сведения

Архивация и восстановление

Мастер архивации и восстановления (*Backup or Restore Wizard*) создает копию файлов и папок на указанном пользователем носителе информации. В случае потери или повреждения пользовательских данных их можно восстановить из файла резервной копии. Специалисты рекомендуют выполнять регулярное создание резервных копий важных файлов и папок. Частота архивации (*резервного копирования*) зависит от частоты изменений файлов, так как в случае потери данных придется повторно создать то, что было сделано после последней архивации. По этой причине многие компании создают резервные копии важных файлов ежедневно. Пользователь может выбирать различные типы архивации в зависимости от его требований.

- Для типа *Обычная (**Normal**)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, и каждый файл маркируется как прошедший архивацию (имеющий резервную копию).
- Для типа *Копирование (**Copy**)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, но файлы не маркируются как прошедшие архивацию.
- Для типа *Добавочная (**Incremental**)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, и каждый файл маркируется как прошедший архивацию.
- Для типа *Разностная (**Differential**)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, но файлы не маркируются.
- Для типа *Ежедневная (**Daily**)* происходит архивация только тех файлов, которые были созданы или изменены в данный день, но файлы не маркируются.

Тип архивации, который применяется, определяет, насколько сложным будет процесс восстановления. Для восстановления после нескольких добавочных

или разностных архиваций необходимо выполнить восстановление из последней обычной резервной копии и из всех добавочных или разностных копий, полученных после обычной архивации и вплоть до настоящего момента. Выполняя архивацию данных, пользователь указываете имя и место для файла резервной копии. По умолчанию файлы резервных копий сохраняются с расширением ***.bkf***. Файлы архивации можно сохранять на жестком диске, на гибком диске или на любом другом типе съемного носителя. При выборе места для резервной копии нужно учитывать размер файла архивации, типы имеющихся носителей, а также возможное требование того, что файлы резервных копий нужно хранить отдельно от компьютера на случай катастрофы.

Функция восстановления системы

Восстановление системы позволяет выполнить откат состояния операционной системы к одной из точек восстановления, фиксирующих состояние на момент, когда система стабильно работала. Преимуществом данной функции заключается в том, что она предоставляет возможность быстрого восстановления ("отката" состояния системы к состоянию, в котором она находилась в один из предыдущих моментов во времени) без переустановки системы, а также не подвергает риску случайного перезаписывания рабочих файлов пользователей. Возможно выполнение отката к любому из следующих типов контрольных точек и точек восстановления.

- *Начальная контрольная точка (**initial system checkpoint**)* системы создается при первом запуске компьютера с вновь установленной ОС.
- Точки восстановления *для автоматических обновлений (**Automatic update restore points**)* создаются, когда инсталлируются обновления, которые загружаются с помощью **Windows Update**.
- Точки восстановления *при восстановлении с резервной копии (**Backup recovery restore points**)* создаются, когда пользователь использует мастер архивации или восстановления (**Backup or Restore Wizard**).
- Пользователь может создавать свои *собственные точки восстановления вручную (**"ручные" контрольные точки - manual checkpoints**)* в любой момент с помощью мастера восстановления системы (**System Restore Wizard**).
- Точки восстановления *при инсталляции программ (**Program name installation restore points**)* создаются, при установке программного обеспечения.
- Точки восстановления *для операции восстановления (**Restore operation restore points**)* создаются каждый раз, когда пользователь осуществляете какое-либо восстановление.

- *Системные контрольные точки (**System checkpoints**)* - это запланированные точки восстановления, которые создаются компьютером регулярно, даже если пользователь не вносил никаких изменений в систему.

- Точки восстановления *для неопознанного устройства (**Unsigned device driver restore points**)* создаются, когда устанавливается драйвер устройства, который не был опознан или сертифицирован.

Средство **Восстановление системы (*System Restore*)** обычно сохраняет набор контрольных точек восстановления за период от одной до трех недель. Количество контрольных точек восстановления, доступных в любой заданный момент времени, ограничено объемом пространства, которое выделено пользователем для работы системы восстановления. Максимальный размер пространства, которое можно выделить, составляет приблизительно 12 процентов.
В ходе процедуры восстановления происходит восстановление ОС и программ, инсталлированных на компьютере, к состоянию, в котором они находились на момент выбранной контрольной точки восстановления. Этот процесс не затрагивает личные файлы пользователя (включая сохраненные документы, сообщения электронной почты, адресную книгу, список **Избранные (*Favorites*)** и список **Журнал (*History*) Internet Explorer**).
Все изменения, внесенные утилитой **Восстановление системы (*System Restore*)**, полностью обратимы, и если пользователя не удовлетворяют результаты, то можно восстановить предыдущие настройки и выполнить все снова.

Архивация и восстановление с помощью программы Cobian Backup

Cobian Backup - бесплатная утилита предназначенная для резервного копирования файлов и папок, которые часто изменяются и имеет более расширенные функции, чем стандартная служба архивации и восстановления Windows. Программа может создавать копии заданных элементов в автоматическом режиме по заданному расписанию.
Cobian Backup может сохранять копии объектов не только на локальном компьютере, но и в локальной сети, на FTP-сервере. При создании резервных копий используется интегрированный zip- и 7-zip-архиватор.
Программа может быть установлена в качестве приложения или как сервис (служба). Для полноценной работы требуется NET Framework 3.5.

Выполнение работы

Задание 1. Выполните резервное копирование системных конфигурационных файлов.

1. Запустите компьютер с предустановленной ОС **Windows**.

2. Запустите **Мастер Архивации (*Пуск → Программы → Стандартные → Служебные → Архивация данных*)**.

3. Ознакомьтесь с информацией мастера и щелкните ***Далее***.

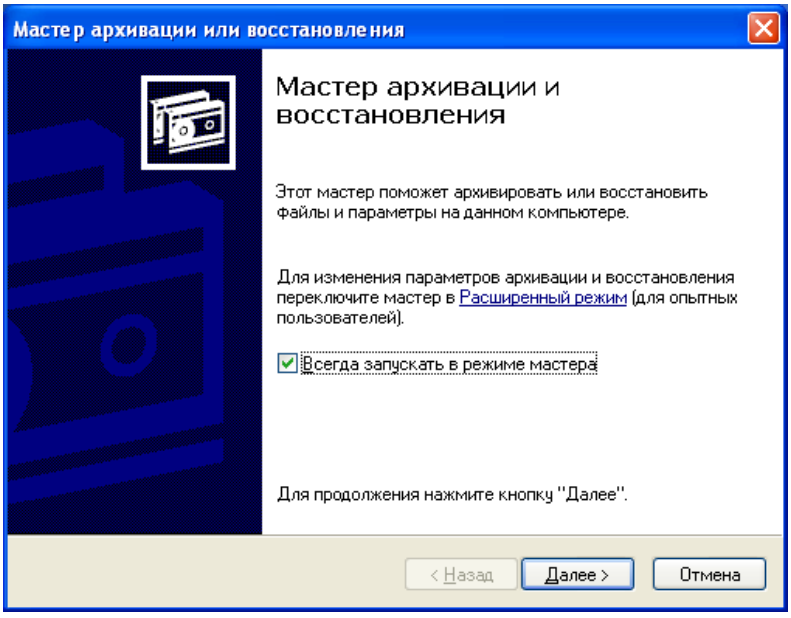


Рисунок 1. Мастер Архивации данных.

4. Выберите возможность мастера – **Архивация файлов и параметров** и щелкните ***Далее***.

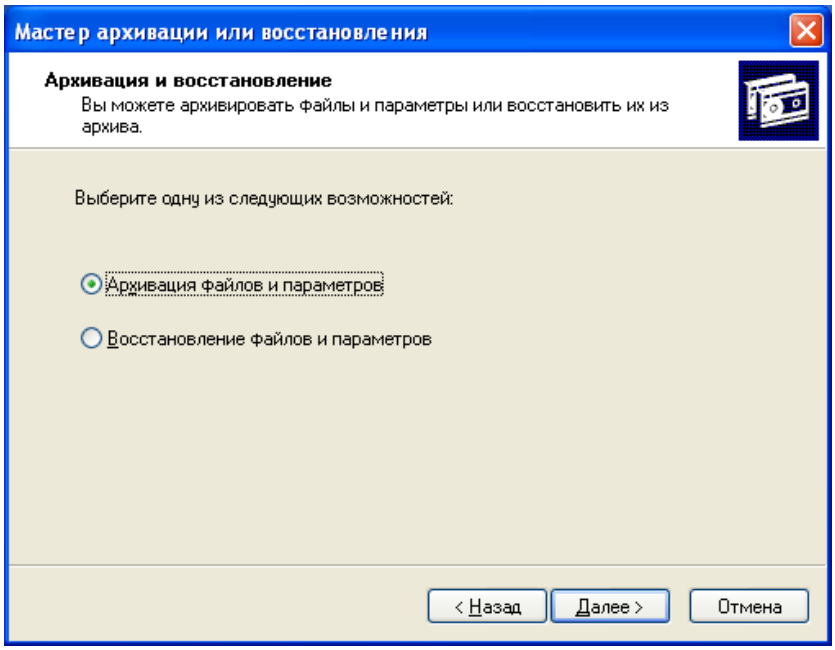


Рисунок 2. Выбор архивации или восстановления.

5. Укажите выбор элементов архивирования в самостоятельном режиме – *Предоставить возможность выбора объектов для архивации* и щелкните ***Далее***.

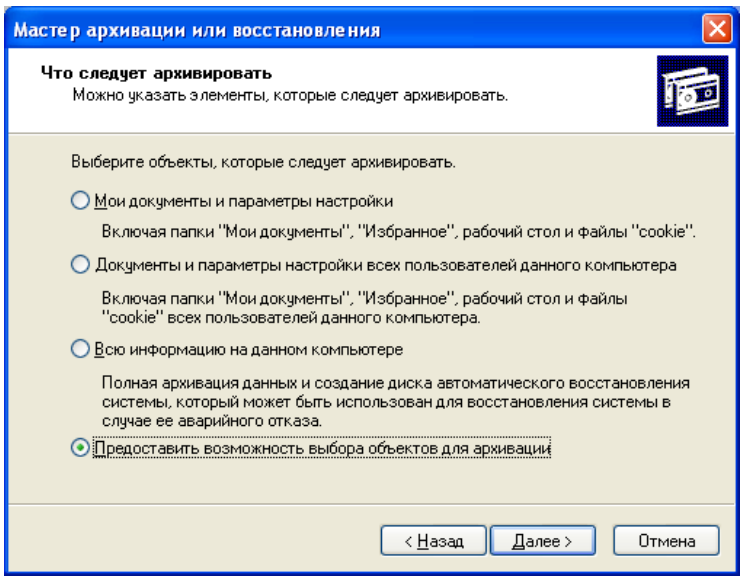


Рисунок 3. Выбор способа указаний объектов архивирования.

6. Укажите элементы для архивации – Выберите на диске D несколько папок общим объем которых не будет превышать несколько мегабайт и щелкните ***Далее***.

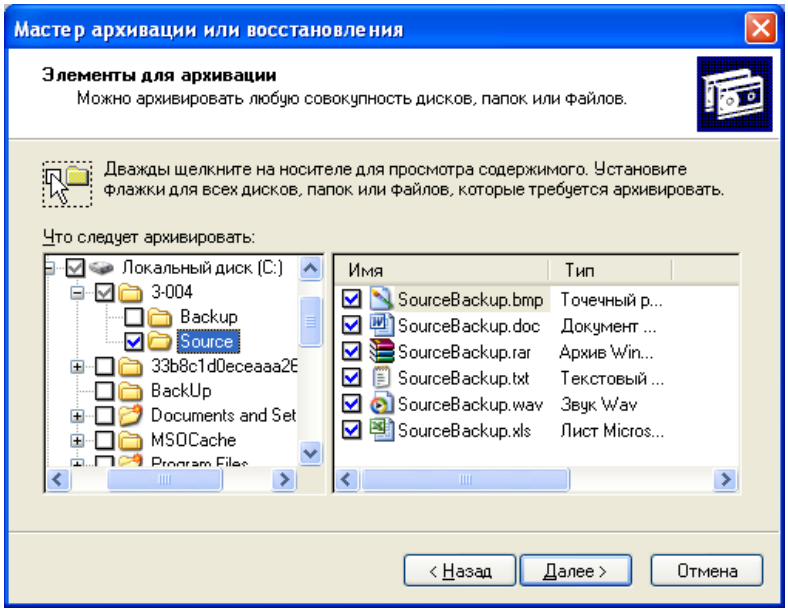


Рисунок 4. Выбор объектов архивирования.

7. Укажите место хранения архива:

   - откройте диалоговое окно **Сохранить** как кнопкой ***Обзор***;

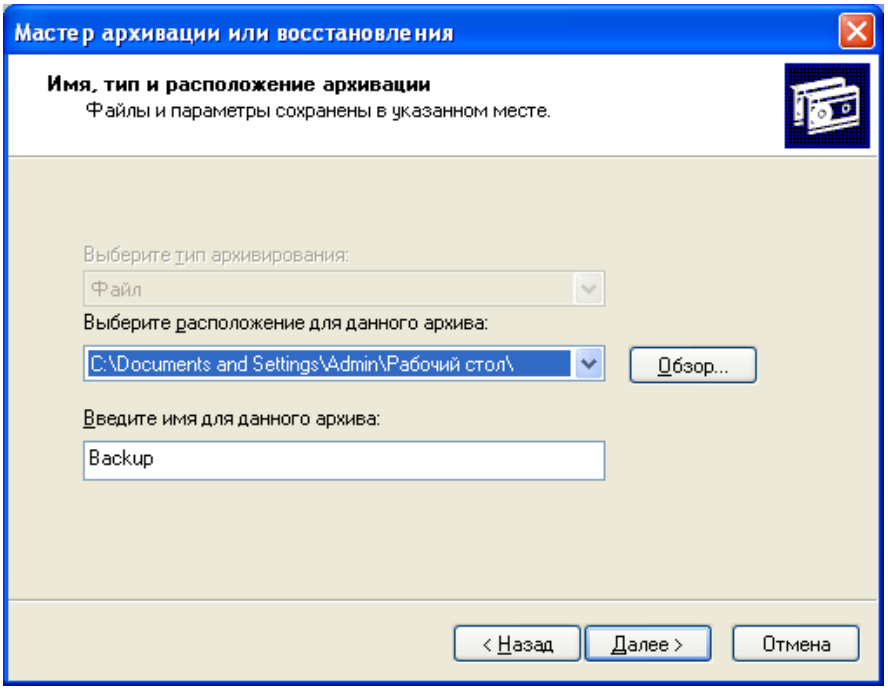


Рисунок 5. Выбор места хранеиня архива.

- перейдите в корневой каталог диска **C**;
- введите в поле **Имя Файла** – имя сохраняемого файла - *Резервная Копия*;
- сохраните файл кнопкой ***Сохранить***;
- подтвердите введенные данные кнопкой ***Далее***.

8. Настройте дополнительные параметры архивации:
   - откройте диалоговое окно дополнительных параметров кнопкой ***Дополнительно***;
   - выберите в раскрывающемся списке **тип архивации** – *Обычный* и щелкните ***Далее***;
   - установите флажок *Проверять данные после архивации* (***Далее***);
   - укажите **способ добавления архива** – *Добавить этот архив к существующему* (***Далее***);
   - укажите **время архивации**:
     - установите радиокнопку *Позднее*;
     - введите имя задания в соответствующее поле;

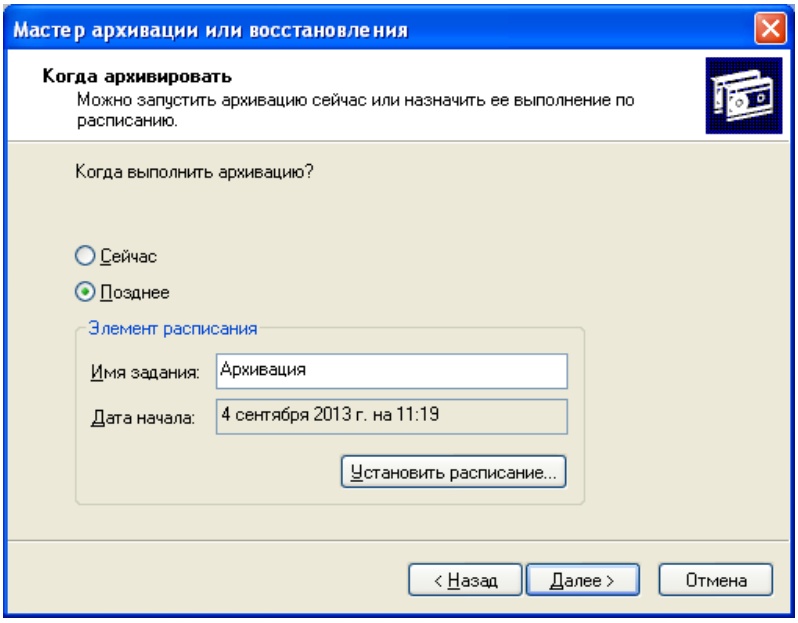


Рисунок 6. Указание имени и времени выполнения архивирования.

- откройте диалоговое окно **Запланированное задание** кнопкой ***Расписание***;

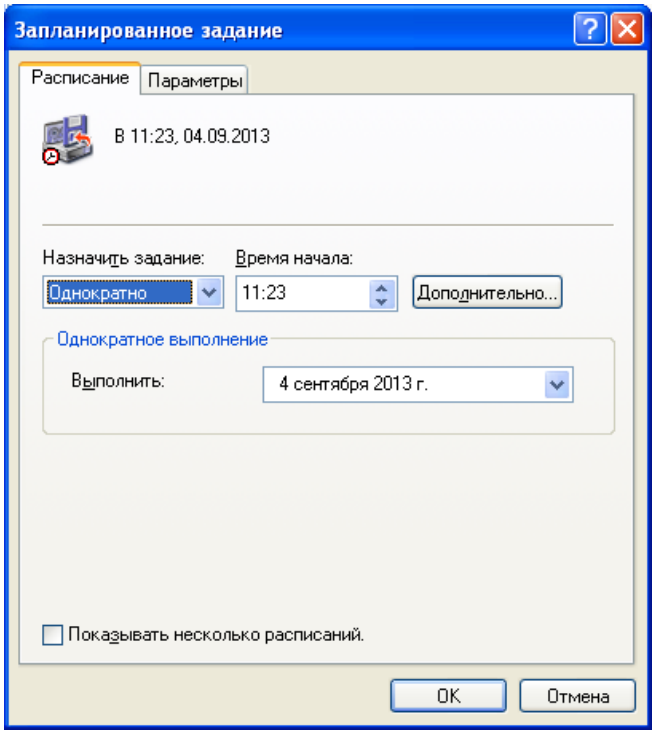


Рисунок 7. Указание точного времени начала выполнения архивирования.

- введите в поле **Время начала** время на *2* минуты позже текущего (например, если сейчас 12.40, то вам необходимо ввести 12.42);

- подтвердите введенные параметры кнопкой ***ОК***;

- завершите ввод времени выполнения архивации кнопкой ***Далее***;
- введите данные пользователя от имени которого будет выполняться архивирование:
  - введите в поле **Пользователь** имя пользователя на компьютере - *USER*;
  - введите в поля **Пароль** и **Подтверждение пароля** для пользователя *USER*;
  - подтвердите ввод данных кнопкой ***ОК***;

9. завершите работу мастера кнопкой ***Готово***.

Задание 2. Выполните восстановление системных конфигурационных файлов.

1. Запустите **Мастер Архивации (*Пуск → Программы → Стандартные → Служебные → Архивация данных*)**.
2. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
3. Выберите возможность мастера – **Восстановление файлов и параметров** и щелкните ***Далее***.
4. Выберите для восстановления в левом списке с содержимым архива, папку ***Мои рисунки*** (***Далее***);.
5. Ознакомьтесь с выбранными параметрами и активизируйте восстановление кнопкой ***Готово***.
6. Откройте отчет кнопкой ***Отчет*** и просмотрите его.
7. Закройте диалоговое окно **Ход восстановления** кнопкой ***Закрыть***.

Задание 3. Создайте точку восстановления.

1. Запустите мастер **Восстановление системы (*Пуск → Программы → Стандартные → Служебные*)**.
2. Ознакомьтесь с информацией мастера.
3. Создайте точку восстановления:
   - Установите радиокнопку *Создать точку восстановления* (***Далее***);
   - введите в текстовое поле **Описание контрольной точки восстановления** - *Тестовая точка восстановления*;

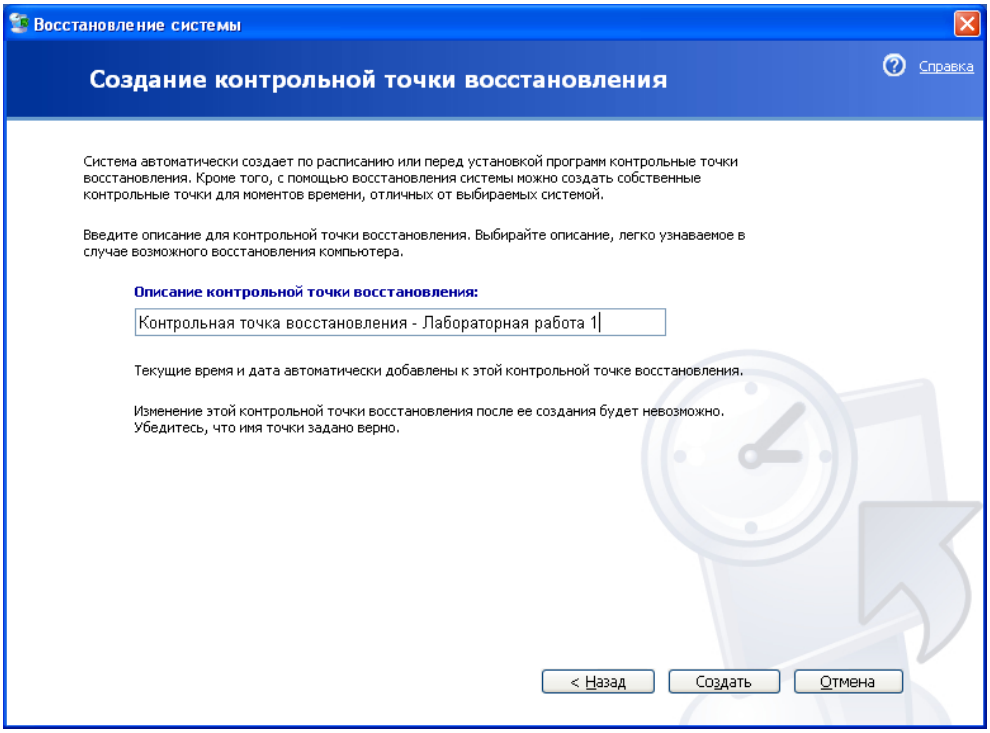


Рисунок 8. Восстановление системы.

- создайте точку восстановления кнопкой ***Создать***.

4. Завершите работу мастера кнопкой ***Закрыть***.

Задание 4. Установите программу Cobian Backup.

1. Для работы программы Cobian Backup необходимо установить на локальный компьютер .NET Framework 3.5. Установочные файл вы можете найти в d:\3-004\Install\dotnetfx35.exe. Запустите данный файл и выполните установку NET Framework 3.5, следуя всем предложенным инструкциям.
2. Запустите программу установки Cobian Backup. Установочный файл находится в той же папке, что и NET Framework 3.5 - d:\3-004\Install\cbsetup.exe.
3. После проверки установочных файлов программа предложит выбрать язык. Выберите из списка «RUSSIAN» и нажмите кнопку «Далее»

Рисунок 9. Окно установщика Cobian Backup.

4. Согласитесь с лицензионным соглашением и нажмите кнопку «Далее».

Рисунок 10. Окно установщика Cobian Backup.

5. Оставьте каталог установки по умолчанию и нажмите кнопку «Далее».

Рисунок 11. Окно установщика Cobian Backup.

6. На этом шаге установки оставьте по умолчанию **Тип установки** – **Служба**, а для **Параметры службы** выберите **Запускать под учетной записью Local system**. Нажмите кнопу «Далее».

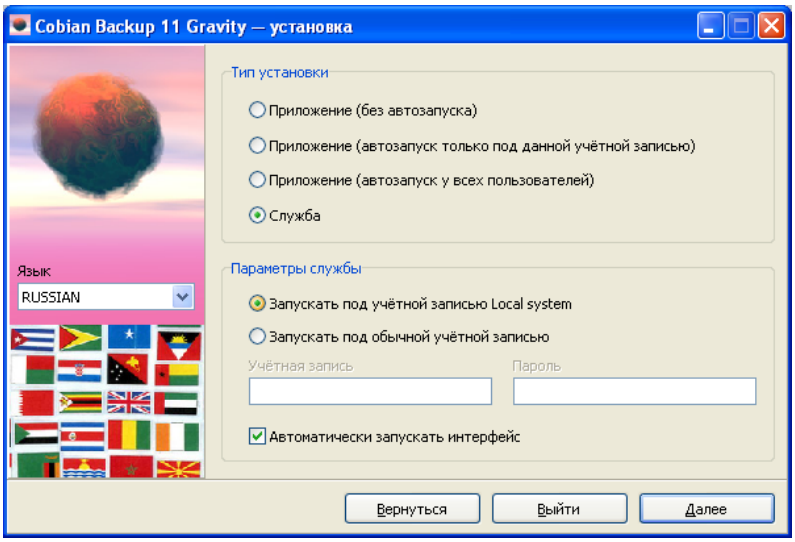


Рисунок 12. Окно установщика Cobian Backup.

7. Нажмите кнопку «Установить».

Задание 5. Выполните резервное копирование с помощью программы Cobian Backup.

1. Запустите программу Cobian Backup.
2. Ознакомьтесь с интерфейсом программы и создайте **Новое задание** (**Задание → Новое задание**).

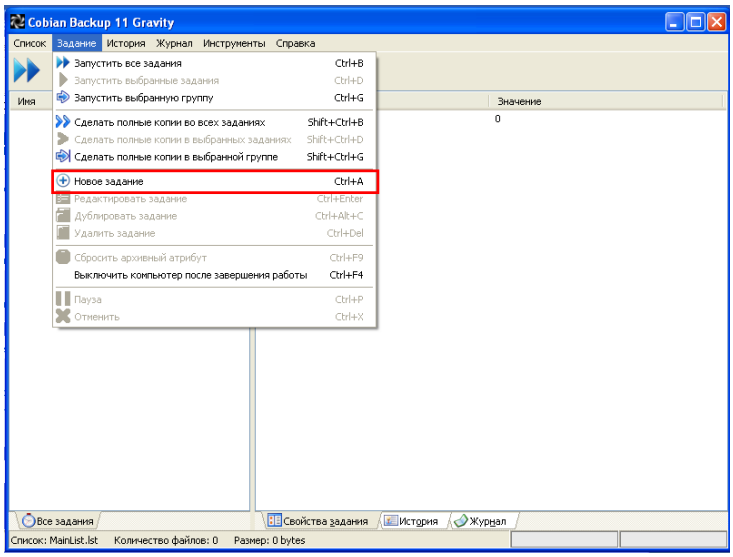


Рисунок 13. Окно программы Cobian Backup.

3. Перед вами появится окно настройки нового задания с открытой вкладкой **Общие**. На это вкладке укажите Название для задания и выберите **Тип копирования** – **Полный**.

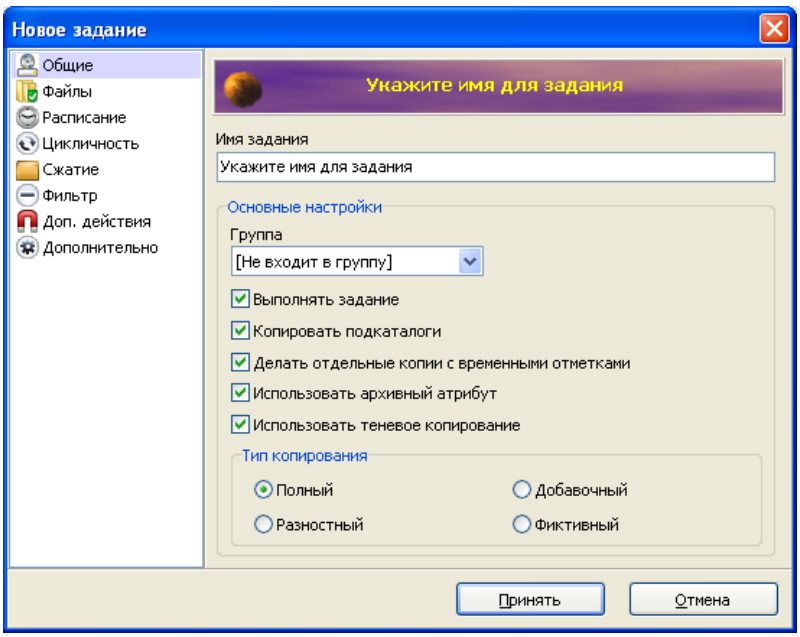


Рисунок 14. Окно Нового задания Cobian Backup. Вкладка Общие.

Варианты "Тип копирования" позволяют определить, будут ли файлы копироваться в полном объеме или только обновляться.

- **Полный** — все файлы указанной папки будут включены в резервную копию. Если выше включена опция "Создавать отдельные копии...", всякий раз будут сохраняться новые файлы с резервной копией. Если опция "Создавать отдельные копии..." отключена, будет обновляться один и тот же файл (поверх старой версии).
- **Добавочный** — в новую резервную копию будут включены только те файлы, которые изменились со времени создания последней резервной копии (не забудьте отметить опцию "Использовать архивный атрибут").
- **Разностный** — только файлы, которые изменились со времени последнего полного резервного копирования.
- **Фиктивный** — ничего не копируется, задание используется для дополнительных действий.

4. Перейдите на вкладку **Файлы**. Верхняя часть окна **Источники** предназначена для файлов, которые мы хотим включить в резервную копию. Перенесите сюда прямо из проводника (или используйте кнопку Добавить) каталог d:\3-004\Source.
   Нижняя часть окна **Пути назначения** предназначена для указания местоположения резервной копии. Укажите в качестве пути назначения каталог d:\3-004\Backup.

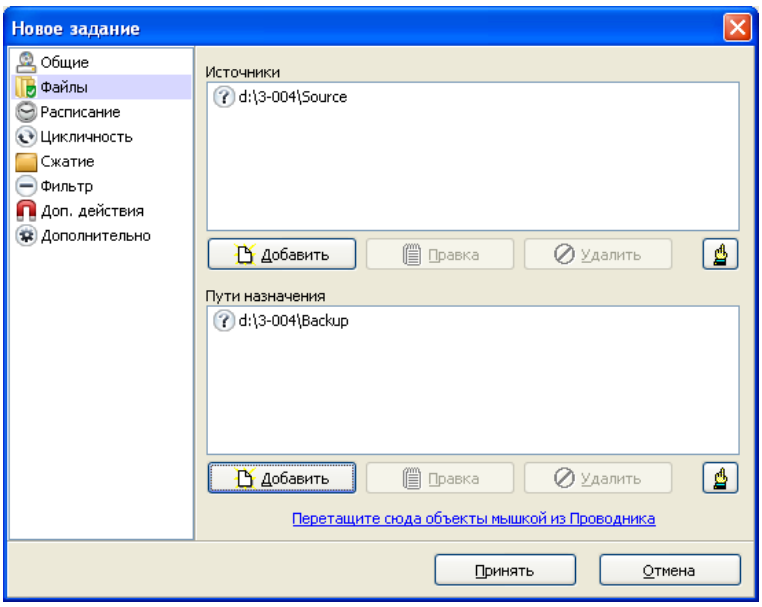


Рисунок 15. Окно Нового задания Cobian Backup. Вкладка Файлы.

5. Перейдите во вкладку **Расписание**. Изучите предложенные варианты расписаний для резервного копирования и выберите в списке **Схема запуска - Еженедельно**. Укажите в группе **Дни недели**: **Понедельник** и **Среда**, а в группе **Дата и время** укажите в поле **Время** 12:00:00.

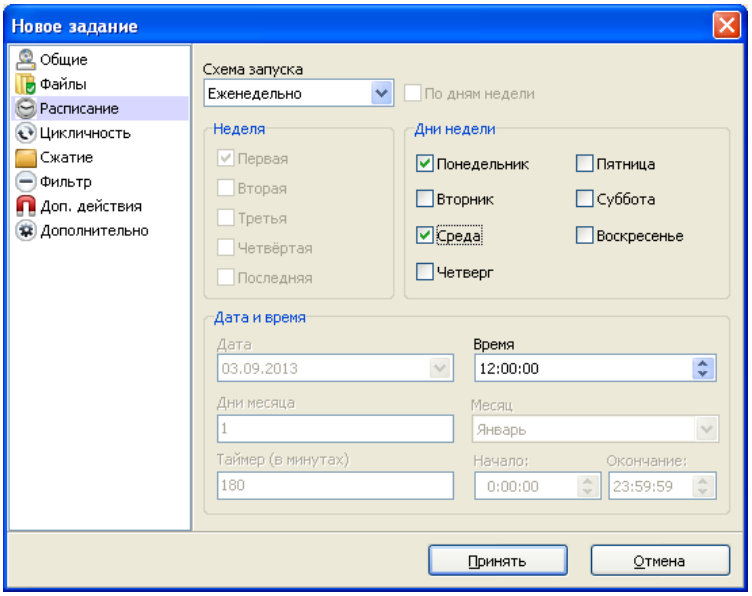


Рисунок 16. Окно Нового задания Cobian Backup. Вкладка Расписание.

6. Перейдите во вкладку **Сжатие**. В списке **Тип сжатия** выберите тип архива **Zip**. В поле Комментарий укажите комментарий, который будет добавлен к архиву. Для того, чтобы защитить архив от чужих посягательств – зашифруйте его. Выберите из списка **Вид шифрования** – **AES 256 бит**. Для шифрования архива придумайте достаточно сложную секретную фразу (которая будет известна только вам) и укажите ее в поле **Секретная фраза**. Повторно укажите данную фразу в поле **Подтверждение секретной фразы**. Для определении сложности секретной фразы предусмотрен специальный индикатор, который в

нашем случае должен быть зеленого цвета (это значит, что секретная фраза достаточно устойчива ко взлому).

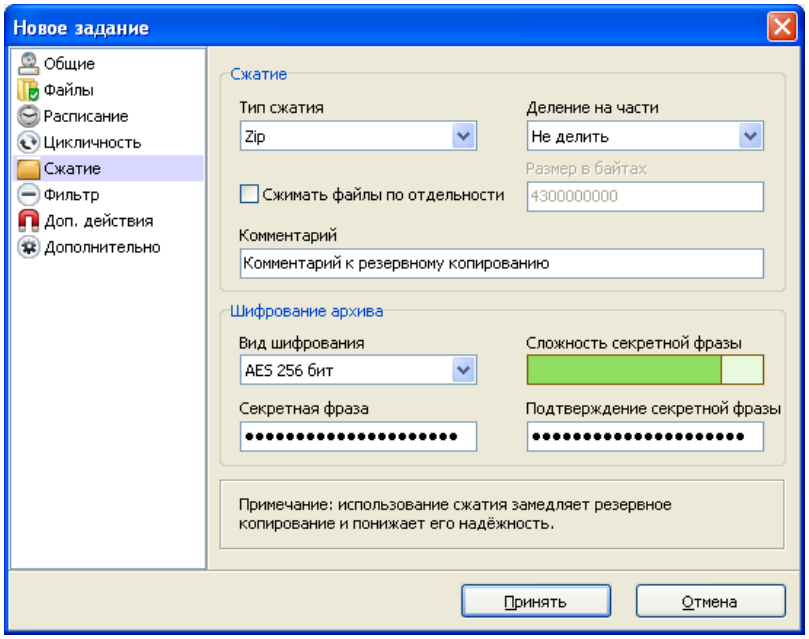


Рисунок 17. Окно Нового задания Cobian Backup. Вкладка Сжатие.

7. Нажмите кнопку **Принять** и запустите созданное вами задание.

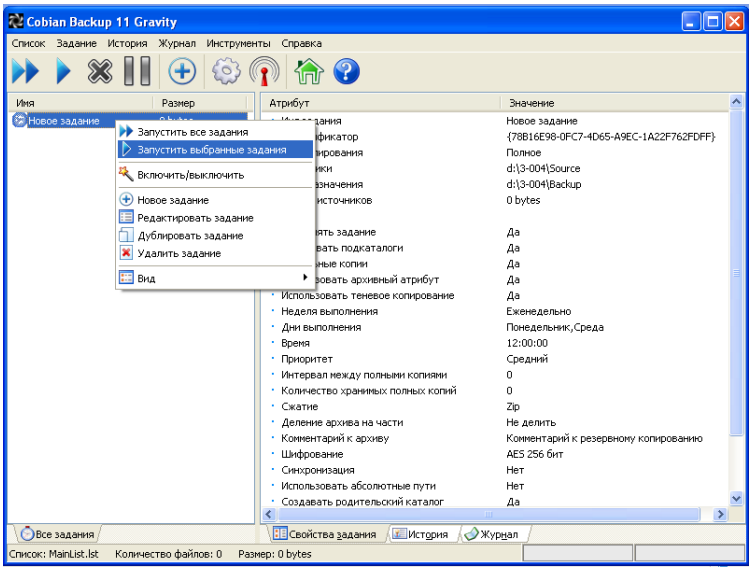


Рисунок 18. Запуск задания в Cobian Backup.

Задание 6. Восстановите данные из резервной копии.

Выполнить данное задание можно несколькими способами:

1. Разархивировать резервную копию можно любой программой поддерживающей работу с выбранным вами типом архива и типом шифрования.
2. Разархивировать резервную копию с помощью встроенного в Cobian Backup инструмента **Распаковщик**.

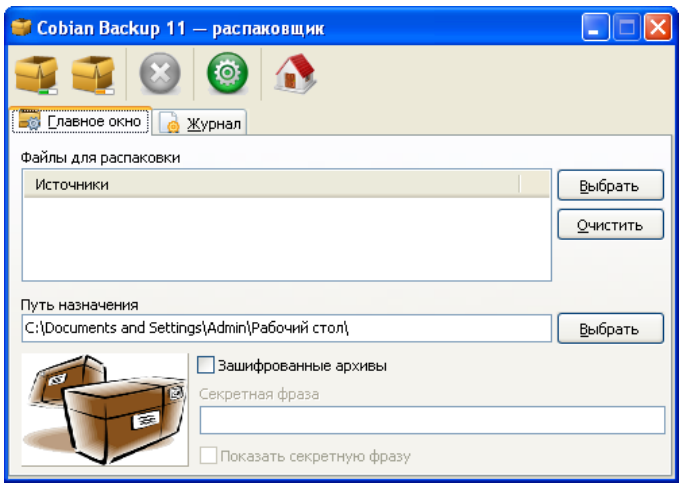


Рисунок 19. Окно Распаковщика в Cobian Backup.

Задание 5. Выполните резервное копирование на удаленный сервер с помощью программы Cobian Backup.

Измените настройки созданного вами задания резервного копирования так, чтобы ваша резервная копия сохранялась на удаленном FTP-сервере.

1. В окне настроек задания резервного копирования зайдите на вкладку **Файлы** и измените **Пути назначения,** выбрав для местоположения резервной копии **FTP**.

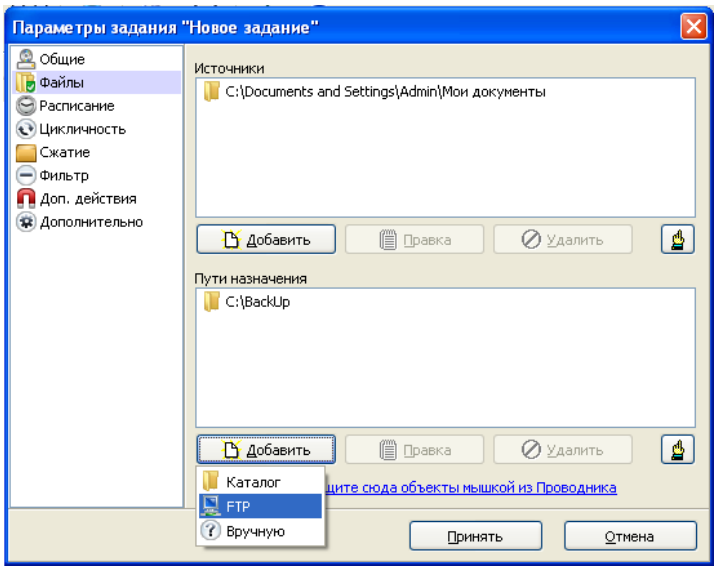
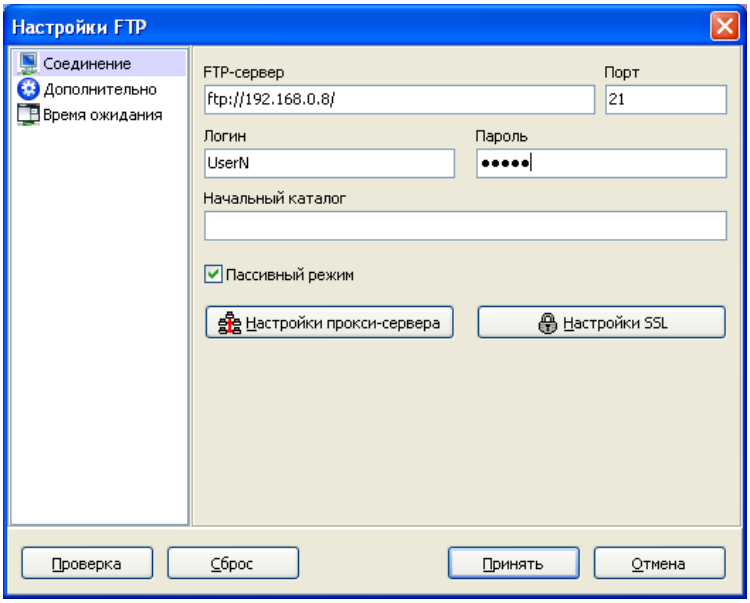


Рисунок 9. Окно параметров Нового задания Cobian Backup. Вкладка Файлы.

2. В появившемся окне «**Настройки FTP**» в поле FTP-сервер введите ftp://192.168.1.23/. В поле **Имя пользователя** укажите **UserN** (где N – ваш порядковый номер в журнале). В поле Пароль укажите такое же значение как и для поля Имя пользователя. Остальные настройки оставьте без изменения.



3. Сохраните изменения для задания резервного копирования и запустите его.
4. По окончанию резервного копирования зайдите через любой файловый менеджер на FTP-сервер и убедитесь, что резервная копия создана.

Содержание отчета

Отчет по лабораторной работе предоставляется преподавателю в электронном виде и должен содержать:

1. Титульную страницу (стандартное оформление).
2. Описание основных заданий, выполняемых в ходе лабораторной работы.
3. Скриншоты. В скриншотах диалоговых окон, в которых курсант должен указать название или комментарий к резервным копим или точкам восстановления системы, обязательно должна присутствовать в скобках фамилия курсанта, выполнявшего данную лабораторную работу.

Вопросы для защиты лабораторной работы

1. Зачем необходимо выполнять резервное копирование данных?
2. Какие существуют типы архивации?
3. Как часто необходимо выполнять резервное копирование данных.

Лабораторная работа № 9

Исследование настройки системы безопасности

Цель работы: Изучить настройки системы безопасности

Теоретическая часть:

Установка ограничений для пользователей

Группы опций в окне Default User предназначены для установки доступности пользователю различных возможностей рабочего стола Windows NT 4.0

Установка ограничений на компьюте

Группы опций в окне Default Computer предназначены для установки доступности пользователю различных возможностей по конфигурации аппаратного обеспечения и среды самой Windows NT 4.0

Прямое редактирование системного регистра

С помощью Редактора Системной Политики можно не только создавать файлы политики, но и напрямую редактировать системный регистр своего (с помощью команды **Open** Registry) или чужого (с помощью ко-
манды **Connect)** компьютера. При этом изменения, вносимые вами в Редакторе Системной Политики, немедленно отражаются в системном регистре. Однако к этой возможности следует относиться с большой осторожностью, как и ко всем исправлениям в системном регистре.

Запрет использования USB-накопителей для отдельных групп пользователей (Win Vista, Win 7)

Самое простое решение для ограничения бесконтрольного использования внешних USB-накопителей в операционных системах Windows Vista и Windows 7 – это полное отключение возможности их использования для отдельных групп пользователей. Для этого необходимо изменить параметры безопасности для двух файлов USBSTOR.PNF USBSTOR.INF, которые расположены в папке %systemroot%\INF. Чтобы запретить установку USB-устройств, необходимо изменить параметры безопасности для каждого из этих файлов. Для этого правой кнопкой мыши щелкаем на выбранном файле, выбираем «Свойства», затем вкладку «Безопасность», выбираем на ней группы, к которой принадлежит пользователь (для которого необходимо запретить установку USB-накопителей) и затем выбираем опцию «Запретить – Полный доступ» (рисунок 1). Этот способ работает для накопителей ранее не подключавшихся к компьютеру.

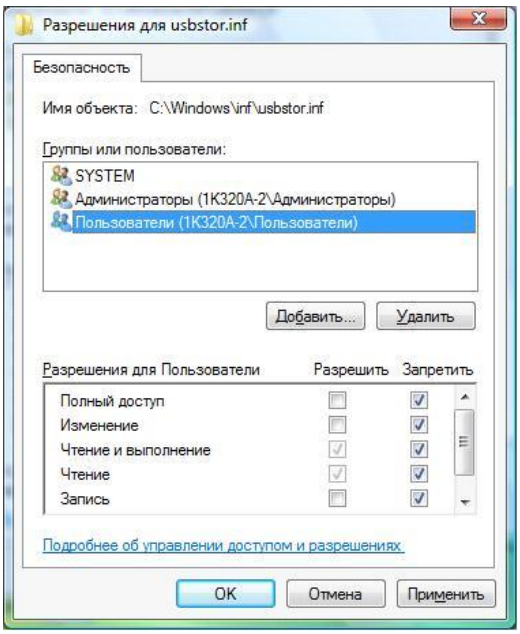


Рисунок 1 – Настройка группы пользователей на запрещение полного доступа к файлу usbstor.inf

Запрет использования USB-накопителей через реестр (Win XP, Win Vista, Win 7)

Запрет на использование USB-накопителей можно осуществить и через реестр. Для этого потребуется изменить ветку HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR, где параметру Start необходимо присвоить значение «4». Для этого в редакторе реестра regedit выбираем нужную ветку, выделяем указателем мыши USBSTOR, находим параметр Start, выделяем его, нажимаем правую кнопку, выбираем «Изменить» и в появившемся окне вводим новое значение (рисунок 2). Теперь при подключении к компьютеру USB-накопитель работать не будет. Этот способ работает только для тех накопителей, которые были уже установлены в компьютер ранее. При установке нового накопителя измененный параметр вернет свое ранее установленное значение – «3». Для того, чтобы внесенные в реестр изменения вступили в силу перезагрузка компьютера не требуется.

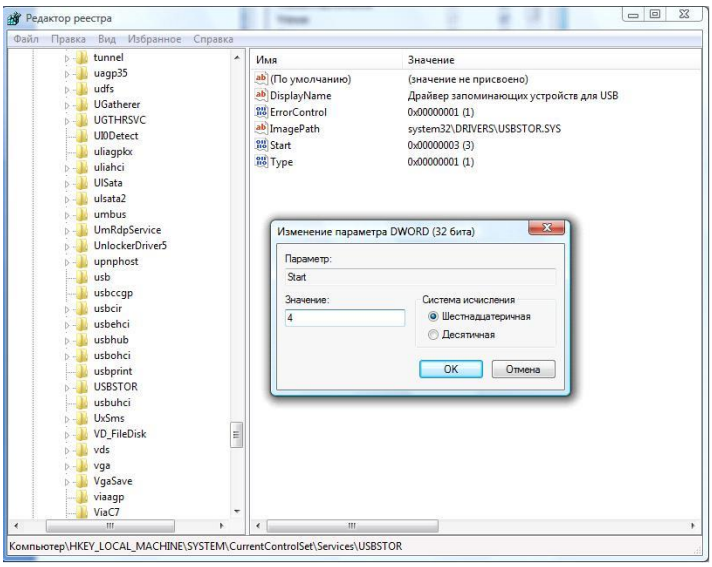


Рисунок 2 – Изменение значения параметра Start в ветке HKLM\SYSTEM\CurrentControlSet\Services\USBSTOR

Запрет записи на USB-накопители через реестр (Win XP, Win Vista, Win 7)

Для запрета записи информации на съемные носители необходимо в значение параметра WriteProtect в ветке реестра HKLM\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies установить в «1». Тогда в случае попытки записи на съемный носитель пользователь получит предупреждение. Раздел StorageDevicePolicies и параметр WriteProtect может отсутствовать в реестре, поэтому для использования предложенного способа необходимо их создать и записать нужное значение (для запрета записи – «1», для разрешения – «0»).

Для создания раздела необходимо в ветке HKLM\SYSTEM\CurrentControlSet выбрать указателем мыши Control, нажать правую кнопку, выбрать «Создать», далее выбрать «Раздел» и далее созданный раздел переименовать в StorageDevicePolicies. Вновь созданный раздел StorageDevicePolicies выделяем указателем мыши, щелкаем правой кнопкой и выбираем «Создать», далее «Параметр DWORD (32 бита)». Полученный параметр переименовываем в WriteProtect и изменяем его содержимое на «1» (рисунок 3). После внесения изменений в этом случае перезагрузка компьютера не требуется.

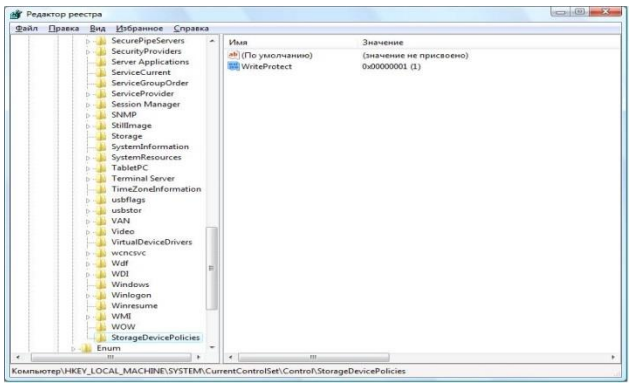


Рисунок 3 – Добавление раздела StorageDevicePolicies и изменение значения параметра WriteProtect

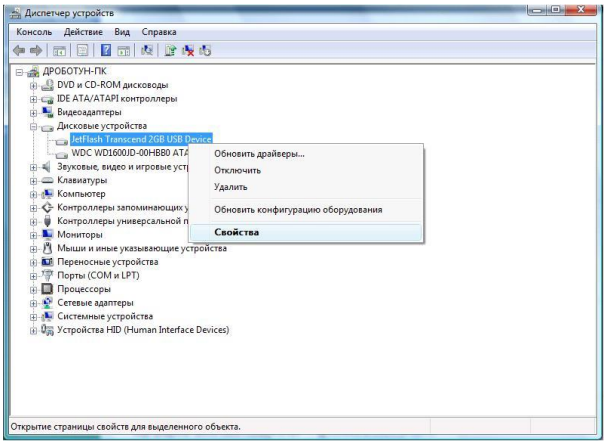


Рисунок 4 – USB-накопитель в «Диспетчере устройств»

4. Указателем мыши выбрать нужный накопитель и нажать правую кнопку, выбрать «Свойства», в результате откроется окно свойств накопителя.

5. Выбираем в открывшемся окне свойств вкладку «Сведения».

6. Выбираем опцию «ИД оборудования» (рисунок 5), и записываем полученный в верхней строке идентификатор USB-накопителя. После этого деинсталлируем накопитель из системы, выбрав в контекстном меню «Удалить». Деинсталляция накопителя необходима для правильной работы политики управления внешними накопителями.

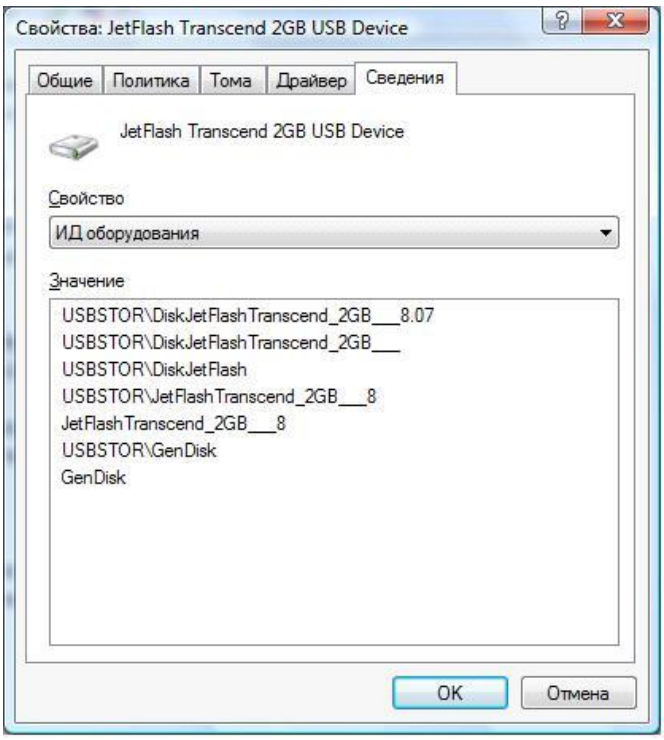


Рисунок 5 – Идентификатор USB-накопителя на вкладке «Сведения» окна «Свойства»

Используя полученный идентификатор USB-накопителя можно создавать и настраивать политики управления внешними накопителями. Для правильной работы политики управления внешними накопителями, необходимо произвести деинсталляцию всех ранее установленных в системе внешних USB-накопителей. Это можно сделать с помощью утилиты USBDeview

Для создания списка разрешенных к установке внешних накопителей, необходимо для всех разрешенных накопителей получить описанным выше способом идентификаторы и настроить для них групповую политику:

1. Из меню «Выполнить» запускаем редактор групповой политики gpedit.msc (рисунок 6).

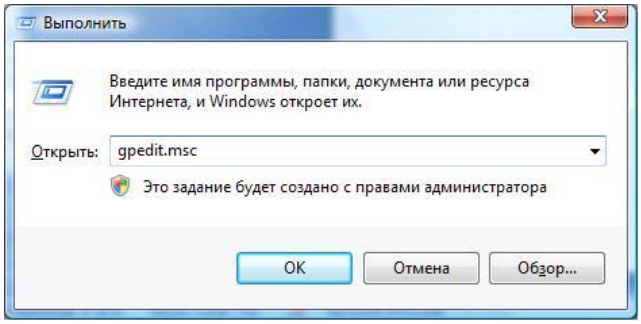


Рисунок 6 – Запуск редактора групповых политик

2. В открывшемся редакторе групповых политик разворачиваем «Конфигурация компьютера», «Административные шаблоны», «Система», «Установка устройства», «Ограничение на установку устройств» и выбираем «Разрешить установку устройств соответствующих какому-либо из этих кодов устройств»(рисунок 7).

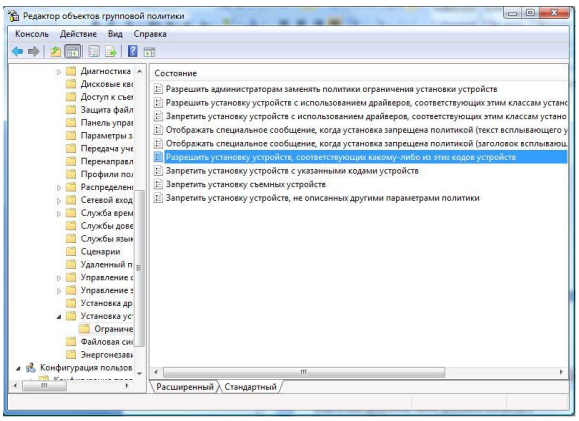


Рисунок 7 – Редактор объектов групповой политики

3. Правой кнопкой мыши нажимаем на выбранной опции «Разрешить установку устройств соответствующих какому-либо из этих кодов устройств» и выбираем «Свойства».

4. Нажимаем «Включен», затем показать и в открывшемся диалоговом окне «Добавить».

5. Вписываем в появившемся окне идентификатор накопителя (рисунок 8).

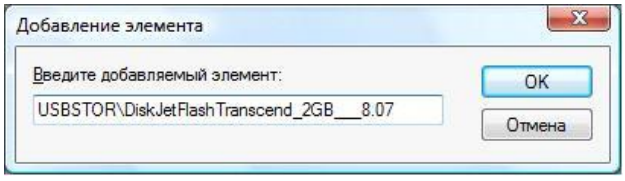


Рисунок 8 – Добавление идентификатора внешнего накопителя в список разрешенных устройств

6. Таким же образом добавляем в список разрешенных устройств остальные идентификаторы.

7. Выбираем в редакторе групповых политик «Запретить установку устройств, не описанных другими параметрами политики», нажимаем правую кнопку мыши, выбираем «Свойства» и нажимаем «Включен».

8. Сохраняем все параметры политики и выходим из редактора.

Таким образом, мы сформировали список разрешенных к установке внешних USB-накопителей и настроили политику их контроля.

Можно пойти дальше и настроить собственное оповещение. Для этого существуют две политики «Отображать специальное сообщение, когда установка запрещена политикой (текст всплывающего уведомления)» и «Отображать специальное сообщение, когда установка запрещена политикой (заголовок всплывающего сообщения)».

Запрет автозапуска файла AUTORUN.INF при подключении внешних носителей (Win XP, Win Vista, Win 7)

1. Отключаем автозапуск стандартными средствами Windows Vista. Заходим в «Панель управления», далее выбираем «Автозапуск» и снимаем галочку с «Использовать автозапуск для всех носителей и устройств».

2. В Windows XP запускаем редактор групповых политик и преходим в «Конфигурация компьютера», «Административные шаблоны», «Система». Находим в правом окне «Отключение автозапуска» и нажимаем «Включен».

3. Изменяем ключ реестра, отвечающий за автозапуск с CD или DVD привода. Заходим в редактор реестра regedit, переходим в ветку HKLM\System\CurrentControlSet\Services\cdrom и устанавливаем параметр AutoRun равным «0» (рисунок 9).

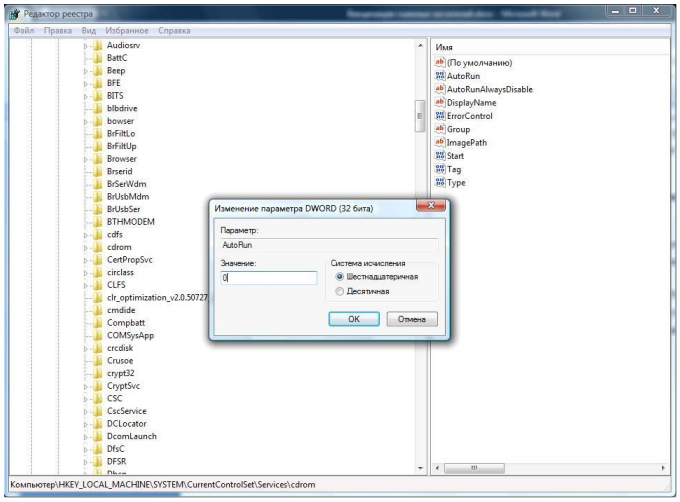


Рисунок 9 – Изменение ключа реестра, отвечающего за автозапуск с CD и DVD

4. Создаем новый ключ NoDriveTypeAutoRun типа dword в ветке HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer и задаем его значение равным «ff» в шестнадцатеричной системе (рисунок 10).

5. Обновляем параметры файлов, для которых не будет работать автозапуск, добавив в них в них маску *.*. В разделе HKLM\SOFTWARE\ Microsoft\Windows\CurrentVersion\explorer\AutoplayHandlers\CancelAutoplay\ Files создаем строковой параметр типа REG_SZ с названием *.* (рисунок 11).

Также есть весьма простой способ не выполнять автозапуск файлов со сменных носителей при их подключении к компьютеру. Необходимо перед подключением внешнего носителя нажать и удерживать клавишу «SHIFT» и отпустить ее после того как внешнее устройство будет установлено. При этом

открывать установленный диск необходимо не двойным щелчком указателем мыши по иконке, а через контекстное меню, выбрав «Проводник».

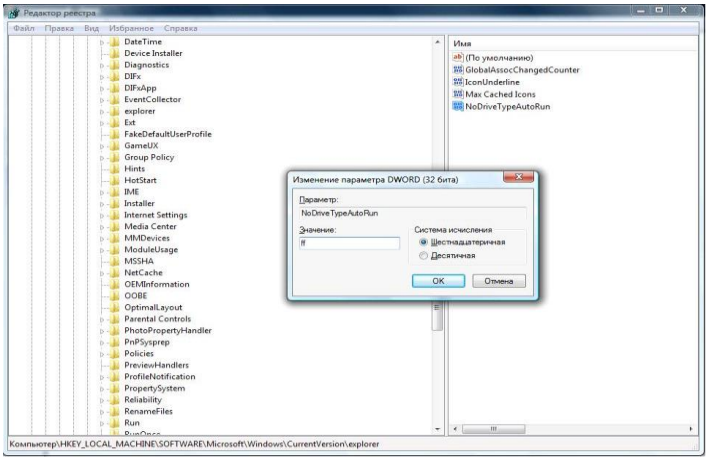


Рисунок 10 – Новый ключ NoDriveTypeAutoRun в ветке HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\explorer

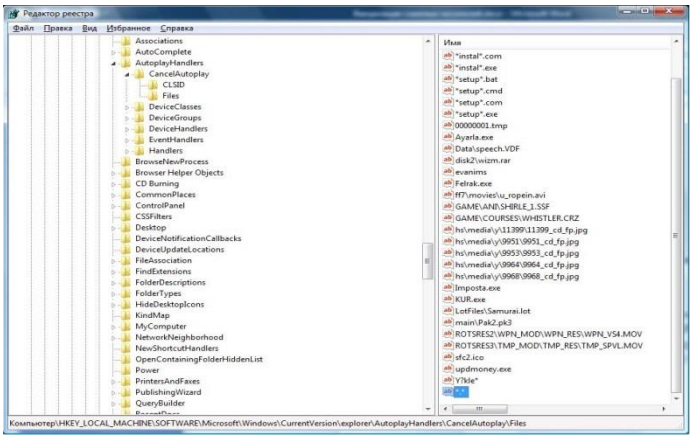


Рисунок 11 – Добавление маски *.* в список файлов, для которых не будет работать автозапуск

Исключение возможности записи файла AUTORUN.INF на USB-накопитель, использующий файловую систему NTFS

Для реализации этого способа необходимо отформатировать USB-накопитель в NTFS, далее в корневом каталоге создаем папку, в которой будет храниться вся информация, записываемая на этот носитель. Имя этой папки может быть любым. Чтобы исключить возможность записи файла AUTORUN.INF и файла содержащего тело вируса, необходимо запретить запись в корневой каталог, оставив при этом возможность записи в папку, которую мы создали ранее. Для этого выделяем созданную папку указателем мыши, нажимаем правую кнопку, выбираем «Свойства» и вкладку «Безопасность», нажимаем на «Дополнительно», в появившемся окне

нажимаем «Изменить» и снимаем галочку с «Добавить разрешения, наследуемые от родительских объектов» (рисунок 12).

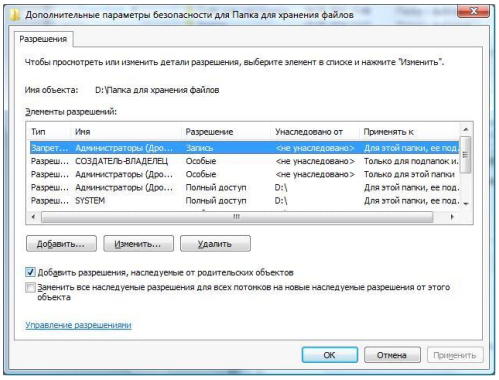


Рисунок 12 – Отключение наследования разрешений для выбранной папки

Мы получили USB-накопитель на который не может записаться файл AUTORUN.INF и сам вирус. При этом всю информацию необходимо сохранять в предварительно созданной папке. Также следует помнить, что при извлечении из компьютера носителей отформатированных в NTFS необходимо обязательно использовать «Безопасное извлечение устройства».

Задание 1. Установить ограничения на компьютер
Задание 2. Запретить использование USB-накопителей
для отдельных групп пользователей
Задание 3. Запретить запись на USB-накопитель через реестр
Задание 4. Запретить автозапуск файла AUTORUN.INF при подключении внешних носителей

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод

Лабораторная работа № 10

Исследование развертывание службы печати

Цель работы: Ознакомиться с развертыванием службы печати

Теоретическая часть:

Службы печати

Службы печати позволяют совместно использовать принтеры в сети, а также централизировать задачи управления сервером печати и сетевым принтером. Кроме того, они позволяют переносить серверы печати и выполнять развертывание подключений к принтерам с помощью групповой политики. Дополнительные сведения приведены в разделе Обзор управления печати в справке Windows Server 2008 R2.

- Назначение: Windows Server 2008 R2

Для защиты сервера печати следует учитывать, какими правами обладают пользователи и группы. Можно защитить сервер печати, предоставив определенные права пользователям и группам. Каждому пользователю или группе можно предоставлять права для выполнения следующих действий:

- Печать документов.
- Управление принтерами.
- Операции по управлению документами.
- Просмотр сведений о сервере печати.
- Управление сервером печати.
- Использование специальных разрешений и дополнительных параметров.

Установка разрешений для серверов печати

1. Откройте «Управление печатью».
2. В левой области щелкните **Серверы печати**, щелкните правой кнопкой нужный сервер печати и выберите **Свойства.**
3. На вкладке **Группа безопасности** в разделе **Группы или пользователи** выберите пользователя или группу, для которой нужно настроить разрешения.
4. В разделе **Разрешения для** <*user or group name*> установите флажок **Разрешить** или **Запретить** напротив соответствующих разрешений.
5. Чтобы изменить **Особые разрешения**, щелкните **Дополнительно.**
6. На вкладке **Разрешения** выберите пользовательскую группу и нажмите кнопку **Изменить.**
7. В диалоговом окне **Запись разрешений** установите флажки **Разрешить** или **Запретить** для разрешений, которые нужно изменить.

Основные сведения о средстве "Управление печатью"

Оснастка "Управление печатью" на компьютерах с системами Windows Vista Business, Windows Vista Enterprise, Windows Vista Ultimate и Windows Server 2008 доступно из папки "Администрирование". Это средство

используется для установки, просмотра всех принтеров и серверов печати Windows в организации, а также для управления ими.

Средство "Управление печатью" предоставляет текущие сведения о состоянии принтеров и серверов печати в сети. Оно позволяет установить подключение к принтеру одновременно для группы клиентских компьютеров и удаленно просматривать состояние очереди печати. Реализованные в этом средстве фильтры помогают выявить ошибки в работе принтеров. Можно также настроить отправку уведомлений по электронной почте или выполнение сценариев при возникновении необходимости обслуживания принтера или сервера печати. Для принтеров, оснащенных веб-интерфейсом, средство "Управление печатью" может отображать более подробные данные, например сведения о наличии тонера и бумаги.

Примечание

Для управления удаленным сервером печати необходимы права члена группы "Операторы печати", "Операторы сервера" или локальной группы "Администраторы" удаленного сервера печати. Эти учетные данные не требуются для наблюдения за удаленными серверами печати, но при их отсутствии некоторые функции будут отключены.

Для кого предназначено средство "Управление печатью"

Это руководство предназначено для следующих групп специалистов:

- администраторы печати и специалисты службы поддержки;
- специалисты по планированию ИТ-систем или аналитики, оценивающие продукт;
- специалисты по планированию и проектированию ИТ-систем предприятия.

Преимущества использования средства "Управление печатью"

Средство "Управление печатью" помогает значительно сократить временные затраты администратора печати при установке принтеров на клиентские компьютеры, а также при управлении принтерами и наблюдении за их работой. Задачи, которые ранее выполнялись за десять действий на одном компьютере, теперь выполняются удаленно за два или три действия одновременно для целой группы компьютеров.

Для развертывания подключений принтеров с помощью групповой политики среда должна соответствовать следующим требованиям:

- схема доменных служб Active Directory должна использовать версию Windows Server 2003 R2 или Windows Server 2008;
- на клиентских компьютерах с операционными системами Windows 2000, Windows XP или Windows Server 2003 должно использоваться средство PushPrinterConnections.exe в сценарии запуска (для подключений компьютеров) или входа (для подключений пользователей).

.

Примечание

Средство "Управление печатью" может неточно отображать состояние удаленных компьютеров при наблюдении более чем за 10 серверами печати на компьютере с системой Windows Vista. Это вызвано тем, что компьютеры с системой Windows Vista поддерживают не более 10 одновременных сетевых подключений. Чтобы вести удаленное наблюдение за большим количеством серверов печати, используйте подключение к компьютеру с системой Windows Server 2008, на котором установлено средство "Управление печатью", с помощью удаленного рабочего стола.

. Установка и открытие средства "Управление печатью"

Оснастка "Управление печатью" устанавливается по умолчанию на компьютеры с операционными системами Windows Vista Business, Windows Vista Enterprise и Windows Vista Ultimate, но не устанавливается по умолчанию на компьютеры с системой Windows Server 2008. Для установки средства "Управление печатью" на компьютере с системой Windows Server 2008 используйте один из методов, описанных ниже.

- Установите роль **Службы печати** с помощью мастера добавления ролей диспетчера сервера. При этом происходит установка оснастки "Управление печатью" и настройка сервера печати.
- Установите элемент **Средства служб печати** компонента **Средства удаленного администрирования сервера** с помощью мастера добавления компонентов в диспетчере сервера. При выборе элемента **Средства служб печати** происходит установка оснастки "Управление печатью", но не настройка сервера печати.

Чтобы открыть средство "Управление печатью" на компьютере с Windows Vista или Windows Server 2008, дважды щелкните значок "Управление печатью" в папке "Администрирование".

Примечание

При использовании брандмауэра некоторые или все принтеры сети могут не отображаться в средстве "Управление печатью". Для решения этой проблемы добавьте средство "Управление печатью" в список исключений брандмауэра.

Добавление и удаление серверов печати

Средство "Управление печатью" (Printmanagement.msc) позволяет управлять принтерами, которые работают на серверах печати с системами Windows 2000 и более поздних версий.

Примечание

Для выполнения указанных процедур должна быть установлена роль сервера печати, а пользователь должен быть членом группы "Администраторы".

Добавление серверов печати в средство "Управление печатью"

1. Откройте папку "Администрирование" и дважды щелкните значок **Управление печатью**.

2. В дереве "Управление печатью" щелкните правой кнопкой мыши пункт **Управление печатью** и выберите команду **Добавление и удаление серверов**.

3. В диалоговом окне **Добавление и удаление серверов** в группе **Выбор сервера печати** в разделе **Добавить сервер** выполните одно из указанных ниже действий.

- Введите имя.
- Нажмите кнопку **Обзор**, чтобы найти и выбрать сервер печати.

4. Нажмите кнопку **Добавить в список**.

5. Добавьте необходимое количество серверов печати и нажмите кнопку **ОК**.

Примечание
Чтобы добавить используемый в данный момент локальный сервер, нажмите кнопку **Добавить локальный сервер**.

Удаление серверов печати из оснастки "Управление печатью"

1. Откройте папку "Администрирование" и дважды щелкните значок **Управление печатью**.

2. В дереве "Управление печатью" щелкните правой кнопкой мыши пункт **Управление печатью** и выберите команду **Добавление и удаление серверов**.

3. В диалоговом окне **Добавление и удаление серверов** в группе **Серверы печати** выберите один или несколько серверов и нажмите кнопку **Удалить**.

Для экспорта очередей печати, параметров, портов и управляющих языков принтера и последующего их импорта на другой сервер печати с операционной системой Windows можно использовать мастер переноса принтеров или программу командной строки **Printbrm.exe**. Это является эффективным способом объединения нескольких серверов печати или замены старого сервера.

Примечание
Мастер переноса принтеров и программа командной строки **Printbrm.exe** впервые представлены в системе Windows Vista. Эти средства заменяют Print Migrator 3.1.

Миграция серверов печати

- Миграция серверов печати с помощью оснастки "Управление печатью"
- Миграция серверов печати с помощью командной строки

Миграция серверов печати с помощью оснастки "Управление печатью"

1. Откройте папку "Администрирование" и щелкните значок **Управление печатью.**
2. В дереве "Управление печатью" щелкните правой кнопкой мыши компьютер с очередями печати, которые требуется экспортировать, и выберите команду**Экспортировать принтеры в файл**. Откроется **мастер переноса принтеров.**
3. На вкладке **Выберите расположение файла** задайте место сохранения параметров принтера и нажмите кнопку **Далее** для сохранения принтеров.
4. Щелкните правой кнопкой мыши компьютер, на который импортируются принтеры, и выберите команду **Импортировать принтеры из файла**. Откроется**мастер переноса принтеров.**
5. На вкладке **Выберите расположение файла** укажите расположение файла параметров принтера и нажмите кнопку **Далее.**
6. На вкладке **Выберите параметры импорта** задайте следующие параметры:
   - **Режим импорта**. Определяет действия при наличии указанной очереди печати на конечном компьютере.
   - **Внести в Active Directory**. Указывает на необходимость публикации импортированной очереди печати в доменных службах Active Directory.
   - **Преобразовать порты LPR в мониторы стандартных портов.** Указывает на необходимость преобразования портов LPR принтера из файлов параметров принтеров в мониторы стандартных портов в процессе импорта принтеров.
7. Нажмите кнопку **Далее**, чтобы импортировать принтеры.

Миграция серверов печати с помощью командной строки

1. Чтобы открыть окно командной строки, нажмите кнопку **Пуск,** выберите пункты **Все программы, Стандартные**, щелкните правой кнопкой мыши пункт**Командная строка** и выберите команду **Запуск от имени администратора**
2. Введите:
3. CD %WINDIR%\System32\Spool\Tools Printbrm -s \\<имя_исходного_компьютера> -b -f <имя_файла>.printerExport
4. Введите:
5. Printbrm -s \\<имя_конечного_компьютера> -r -f <имя_файла>.printerExport

Значение	Описание
<sourcecomputername>	UNC-имя исходного или конечного компьютера

<destinationcomputername>	UNC-имя конечного компьютера
<filename>	Имя файла параметров принтера. Используйте расширения файлов PRINTEREXPORT или CAB.

Примечание
Для просмотра полного синтаксиса этой команды введите в командной строке следующее: Printbrm /?

Развертывание принтеров с помощью групповой политики

Средство "Управление печатью" (Printmanagement.msc) можно использовать с групповой политикой для автоматического развертывания подключений к принтерам для пользователей или компьютеров и установки соответствующих драйверов принтеров. Этот метод установки принтеров удобно использовать в лабораториях, классах или филиалах, где большинство компьютеров или пользователей используют одни и те же принтеры. Кроме того, этот метод полезен при развертывании принтеров для пользователей, не входящих в локальную группу "Администраторы" и использующих компьютеры с системой Windows Vista.

Для развертывания подключений принтеров с помощью групповой политики среда должна соответствовать следующим требованиям:

- схема доменных служб Active Directory должна использовать версию Windows Server 2003 R2 или Windows Server 2008;
- на клиентских компьютерах с операционными системами Windows 2000, Windows XP или Windows Server 2003 должно использоваться средство PushPrinterConnections.exe в сценарии запуска (для подключений компьютеров) или входа (для подключений пользователей).

При развертывании подключений к принтерам с помощью групповой политики используйте следующие разделы:

- Развертывание подключений к принтерам
- Развертывание программы PushPrinterConnections.exe
- Изменение безопасности установки драйверов для принтеров, развернутых с помощью групповой политики

Развертывание подключений к принтерам

При развертывании подключений к принтерам для пользователей или компьютеров с помощью групповой политики используется диалоговое окно **Развертывание с помощью групповой политики** оснастки "Управление печатью". С его помощью подключения к принтерам добавляются в объект групповой политики.

Развертывание принтеров для пользователей или компьютеров с помощью групповой политики

1. Откройте папку "Администрирование" и дважды щелкните значок **Управление печатью**.

2. В дереве **Управление печатью** щелкните объект **Принтеры** в контейнере соответствующего сервера печати.

3. В области результатов правой кнопкой мыши щелкните принтер, который требуется развернуть, и выберите команду **Развертывание с помощью групповой политики**.

4. В диалоговом окне **Развертывание с помощью групповой политики** нажмите кнопку **Обзор**, а затем выберите или создайте новый объект групповой политики для хранения подключений к принтерам.

5. Нажмите кнопку **ОК**.

6. Выберите развертывание подключений к принтерам для пользователей или для компьютеров.

- Чтобы выполнить развертывание для группы компьютеров, то есть предоставить доступ к принтерам всем пользователям этих компьютеров, установите флажок **компьютеров, к которым применим данный объект групповой политики (на компьютер)**.
- Чтобы выполнить развертывание для группы пользователей, то есть предоставить этим пользователям доступ к принтерам с любого компьютера, в систему которого они вошли, установите флажок **пользователей, к которым применим данный объект групповой политики (на пользователя)**.

Примечание
Клиентские компьютеры с системой Windows 2000 не поддерживают подключение к принтерам для компьютера.

7. Нажмите кнопку **Добавить**.

8. При необходимости повторите действия 3–6 для добавления параметров подключения к принтерам в другой объект групповой политики.

9. Нажмите кнопку **ОК**.

Примечание
В случае развертывания для компьютеров система Windows добавляет подключения к принтерам при входе пользователя в систему (или при перезагрузке компьютера, если используется программа PushPrinterConnections.exe). В случае развертывания для пользователей Windows добавляет подключения к принтерам при фоновом обновлении политики (или при входе пользователя в систему, если используется программа PushPrinterConnections.exe). При удалении параметров подключения к принтерам из объекта групповой политики Windows удаляет соответствующие принтеры с клиентского компьютера во время следующего фонового обновления политики или входа пользователя в систему (либо при следующей перезагрузке или входе пользователя в систему, если используется программа PushPrinterConnections.exe).

Развертывание программы PushPrinterConnections.exe

Для развертывания подключений к принтерам с помощью групповой политики на компьютерах с более ранними версиями Windows, чем Windows Vista, необходимо добавить программу PushPrinterConnections.exe в сценарий запуска или сценарий входа пользователя. Программа

PushPrinterConnections.exe считывает параметры подключения к принтерам из групповой политики и добавляет соответствующие подключения к принтерам в учетную запись компьютера или пользователя (или обновляет существующие подключения).

Файл PushPrinterConnections.exe автоматически распознает компьютеры с системами Windows Vista или Windows Server 2008 и прекращает работу. Такие компьютеры по умолчанию поддерживают подключения к принтерам, развернутые с помощью групповой политики, поэтому этот файл можно безопасно развернуть на все клиентские компьютеры организации.

Примечание
В описании следующей процедуры предполагается, что используется интерфейс консоли управления групповыми политиками в системе Windows Server 2008. Для установки консоли управления групповыми политиками в системе Windows Server 2008 используется мастер добавления компонентов диспетчера сервера. При использовании других версий консоли управления групповыми политиками процедура может слегка отличаться.

Добавление файла PushPrinterConnections.exe в сценарии запуска или входа

1. Откройте консоль управления групповыми политиками.
2. В дереве консоли управления групповыми политиками перейдите к домену или подразделению, где хранятся компьютеры или учетные записи пользователей, на которых необходимо развернуть программу PushPrinterConections.exe.
3. Щелкните правой кнопкой мыши объект групповой политики, содержащий подключения принтера, которые требуется развернуть с помощью групповой политики, а затем выберите команду **Изменить.**
4. Перейдите к одному из следующих элементов:
   - если подключения к принтерам развертываются для компьютера – **Конфигурация компьютера**, **Политики**, **Конфигурация Windows**, **Сценарии (запуск/завершение);**
   - если подключения принтера развертываются для пользователя – **Конфигурация пользователя**, **Политики**, **Конфигурация Windows**, **Сценарии (вход/выход из системы).**

Примечание
Клиентские компьютеры с системой Windows 2000 не поддерживают подключение к принтерам для компьютера.

5. Щелкните правой кнопкой мыши пункт **Автозагрузка** или **Вход в систему** и выберите команду **Свойства**.
6. В диалоговом окне **Свойства: Автозагрузка** или **Свойства: Вход в систему** нажмите кнопку **Показать файлы**. Откроется окно **Автозагрузка** или **Вход в систему**.

7. Скопируйте файл PushPrinterConnections.exe из папки %WINDIR%\System32 в окно **Автозагрузка** или **Вход в систему**. Таким образом данная программа будет добавлена к объекту групповой политики и скопирована на остальные контроллеры домена с параметрами групповой политики.

8. В диалоговом окне **Свойства: Автозагрузка** или **Свойства: Вход в систему** нажмите кнопку **Добавить**. Откроется диалоговое окно **Добавление сценария**.

9. В поле **Имя сценария** введите: **PushPrinterConnections.exe**

10. Чтобы включить ведение журнала на клиентских компьютерах с системами Windows Server 2003, Windows XP или Windows 2000 в поле **Параметры сценария**введите: **–log**

Файлы журналов записываются в файл %WINDIR%\temp\ppcMachine.log (при подключениях для компьютера) и %temp%\ppcUser.log (при подключениях для пользователя) на компьютере с примененной политикой.

11. В диалоговом окне **Добавление сценария** нажмите кнопку **ОК**.

12. В диалоговом окне **Свойства: Автозагрузка** или **Свойства: Вход в систему** нажмите кнопку **ОК**.

13. Для связи объекта групповой политики с другими подразделениями или доменами, где необходимо развернуть программу PushPrinterConnections.exe, используется консоль управления групповыми политиками.

Изменение параметров безопасности установки драйверов для принтеров, развернутых с помощью групповой политики

Параметры безопасности по умолчанию в системах Windows Vista и Windows Server 2008 позволяют пользователям, не входящим в локальную группу**Администраторы**, устанавливать только заслуживающие доверия драйверы принтеров, например драйверы, поставляемые с операционными системами Windows или в пакетах драйверов с цифровой подписью.

Чтобы разрешить пользователям, не входящим в локальную группу **Администраторы**, устанавливать подключения к принтерам, развертываемые с помощью групповой политики, и драйверы принтеров без цифровой подписи, необходимо настроить параметры групповой политики "Ограничения указания и печати". Если данные параметры групповой политики не настроены, могут потребоваться учетные данные члена локальной группы **Администраторы**.

Примечание
В следующей процедуре описывается интерфейс консоли управления групповыми политиками в системе Windows Server 2008. Для установки консоли управления групповыми политиками в системе Windows Server 2008 используется мастер добавления компонентов диспетчера сервера. При использовании других версий консоли управления

групповыми политиками процедура может слегка отличаться.

Изменение параметров безопасности установки драйверов для принтеров, развертываемых с помощью групповой политики

1. Откройте консоль управления групповыми политиками.
2. Откройте объект групповой политики, в котором развернуты подключения к принтерам, а затем выберите пункты **Конфигурация пользователя**, **Политики**,**Административные шаблоны**, **Панель управления** и **Принтеры**.
3. Щелкните правой кнопкой мыши пункт **Ограничения указания и печати** и выберите команду **Свойства**.
4. Выберите пункт **Включено**.
5. Снимите следующие флажки:
   - **Функцию указания и печати можно использовать только на следующих серверах**
   - **Функцию указания и печати можно использовать только на компьютерах своего леса**
6. В списке **При установке драйверов для нового подключения** выберите значение **Не показывать предупреждение или запрос на повышение прав**.
7. Прокрутите окно вниз и в списке **При обновлении драйверов для нового подключения** выберите значение **Показывать только предупреждение** .
8. Нажмите кнопку **ОК**.

После настройки этих параметров все пользователи смогут принимать подключения к принтерам и драйверы со своими учетными записями с помощью групповой политики без запросов и предупреждений. Пользователи будут получать предупреждение перед установкой обновленных драйверов с сервера печати, при этом для установки им не потребуется входить в локальную группу **Администраторы**.

Задание 1 Установить разрешение для серверов печати

Задание 2 Добавить сервер печати в средство "Управление печатью

Задание 3 Развертывание принтеров для пользователей или компьютеров с помощью групповой политики

Задание 4. Измененить параметры безопасности установки драйверов для принтеров, развертываемых с помощью групповой политики

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод

Лабораторная работа № 11

Исследование развертывание файловой службы
Роль файловых служб

Цель работы: Изучить развёртывание файловой службы

Теоретическая часть:

- **Управление квотами.** Управление квотами позволяет задавать мягкие или жесткие ограничения размера для томов или дерева папок. Используя стандартные свойства квот, можно создавать и применять шаблоны квот.
- **Управление блокировкой файлов.** Управление блокировкой файлов позволяет определять правила фильтрации, контролирующие или блокирующие попытки сохранить файлы определенных типов в томе или дереве папок. Используя стандартные исключения файлов, можно создавать и применять шаблоны блокировки файлов.
- **Управление отчетами хранилищ.** Управление отчетами хранилищ позволяет создавать встроенные отчеты об использовании квот, управлении блокировкой файлов и схемах использования хранилищ.

Можно также применять политики квот и блокировки файлов при создании общей папки или с помощью интерфейса командной строки.

Для кого предназначена эта возможность

Использование диспетчера ресурсов файлового сервера может оказаться особенно выгодным для специалистов из следующих групп:

- ИТ-администраторы, отвечающие за управление ресурсами сетевых хранилищ данных и желающие эффективно распределять эти ресурсы с помощью квот;
- ИТ-администраторы, желающие исключить возможность хранения файлов определенных типов в сетевых хранилищах;
- ИТ-администраторы, которым необходима возможность создания отчетов для получения более полного представления об использовании серверных ресурсов хранилищ;
- менеджеры по управлению учетными записями пользователей, желающие реализовать политики хранения данных путем создания квот и правил блокировки файлов для пользовательских папок и общих ресурсов хранилищ.

Некоторые дополнительные особенности

Использовать диспетчер ресурсов файлового сервера могут только члены группы администраторов.

Если в организации в настоящее время используются квоты дисков NTFS, благодаря средствам управления квотами, входящими в состав диспетчера ресурсов файлового сервера, управление квотами можно будет сделать более точным (см. приведенную ниже таблицу).

Возможности квоты	Диспетчер ресурсов файлового сервера	Квоты дисков NTFS
Отслеживание квот	По папке или по тому	Для отдельных пользователей тома
Расчет степени использования диска	По фактическому месту на диске	По логическому размеру файлов
Механизмы уведомления	Электронная почта, журналы событий, выполнение команд, встроенные отчеты	Только журналы событий

Квоты, создаваемые в диспетчере ресурсов файлового сервера, не имеют никакого отношения к квотам NTFS: две этих системы работают отдельно друг от друга. Однако для миграции с квот NTFS диспетчер ресурсов файлового сервера предоставляет шаблоны квот, помогающие воссоздать свойства квот NTFS.

Если предполагается использовать диспетчер ресурсов файлового сервера для управления ресурсами хранилищ на удаленном сервере, этот сервер должен работать под управлением системы Windows Server 2008 с диспетчером ресурсов файлового сервера.

Возможности данного компонента

Диспетчер ресурсов файлового сервера в Windows Server 2008 можно использовать для выполнения задач, указанных ниже.

- **Управление квотами**
  - Создание и обновление квот, а также получение сведений о квотах, определяющих ограничения размера для тома или папки.
  - Отправка сообщения электронной почты в список рассылки, регистрация события, выполнение команды или сценария либо создание отчета при достижении предельных показателей хранилища.
  - Определение жесткой квоты, чтобы пользователи не могли превысить ограничение хранилища, или просто отслеживание хранилища для тома или папки.
- **Автоматическое создание квот.** Диспетчер ресурсов файлового сервера можно настроить так, чтобы он применял определенную квоту ко всем существующим вложенным папкам и любым новым вложенным папкам, создаваемым в томе или папке. Например, можно автоматически создавать

стандартные квоты для мобильных пользователей или для новых пользователей в организации.

- **Создание отчетов хранилищ**
  - Выбор подходящего варианта из широкого диапазона встроенных отчетов и задание параметров отчета, специфичных для среды.
  - Составление расписания создания отчетов для определения тенденций использования дисков или частоты блокировки файлов.
  - Немедленное создание отчетов по запросу.
- **Управление удаленными ресурсами.** Можно управлять ресурсами хранилищ на локальном сервере или на удаленном сервере с диспетчером ресурсов файлового сервера.
- **Простое резервное копирование и восстановление параметров**. Конфигурации диспетчера ресурсов файлового сервера хранятся в папке информации системного тома в корневом каталоге сервера и в любом томе, к которому применяются квоты или фильтры блокировки файлов. Для резервного копирования и восстановления конфигураций диспетчера ресурсов файлового сервера можно использовать такое средство резервного копирования, как система архивации данных Windows Server.

Наличие диспетчера ресурсов файлового сервера в разных выпусках системы Windows Server 2008

Диспетчер ресурсов файлового сервера доступен во всех выпусках системы Windows Server 2008, но не входит в число служб установки Server Core ОС Windows Server 2008.

Лабораторная работа № 12

Исследование производительности системы в программе «Диспетчер задач», Мониторинг производительности системы с использованием консоли «Производительность»

Цель работы: научится осуществлять мониторинг производительности системы.

Теоретические часть:

В системе **Windows Server 2003** для просмотра системных журналов можно использовать оснастку ***Event Viewer (Просмотр событий)*** (группа ***Administr-tive Tools (Администрирование)*** на панели управления). Эту оснастку можно также запустить из окна оснастки ***Computer Management (Управление компьютером)***. На рис. 1 показан пример окна оснастки ***Event Viewer*** для контроллера домена.

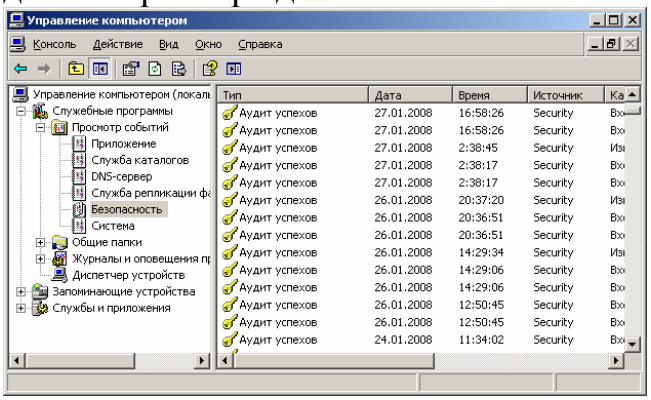


Рисунок. 1. Окно оснастки Event Viewer.

Оснастку ***Event Viewer*** можно также открыть с помощью команды ***Пуск/Программы/Администрирование/Просмотр событий***. С помощью оснастки ***Event Viewer*** можно просматривать три типа стандартных (основных) журналов.

- *Журнал приложений (Application log)* — фиксирует события, зарегистрированные приложениями. Например, текстовый редактор может зарегистрировать в данном журнале ошибку при открытии файла.
- *Журнал системы (System log)* — записывает события, которые регистрируются системными компонентами **Windows Server 2003**. Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы.
- *Журнал безопасности (Security log)* — содержит записи, связанные с системой безопасности. С помощью этого журнала можно отслеживать изменения в системе безопасности и идентифицировать бреши в защите. В данном журнале можно регистрировать попытки входа в систему. Для

просмотра журнала необходимо иметь права администратора. По умолчанию регистрация событий в журнале безопасности отключена.

Помимо стандартных, на компьютере — в первую очередь на контроллере домена — могут быть и другие журналы, создаваемые различными службами (например, ***Active Directory, DNS, File Replication Service*** и т. д.). Работа с такими журналами ничем не отличается от процедур просмотра стандартных журналов.

Журнал системы безопасности может просматривать только пользователь с правами системного администратора. По умолчанию регистрация событий в данном журнале отключена. Для запуска регистрации необходимо установить политику аудита.

Типы событий, регистрирующихся в журналах:

- *Error (Ошибка)* — событие регистрируется в случае возникновения серьезного события (такого как потеря данных или функциональных возможностей). Событие данного типа будет зарегистрировано, если невозможно загрузить какой-либо из сервисов в ходе запуска системы.
- *Warning (Предупреждение)* — событие не является серьезным, но может привести к возникновению проблем в будущем. Например, если недостаточно дискового пространства, то будет зарегистрировано предупреждение.
- *Information (Уведомление)* — значимое событие, которое свидетельствует об успешном завершении операции приложением, драйвером или сервисом. Такое событие может, например, зарегистрировать успешно загрузившийся сетевой драйвер.
- *Success Audit (Аудит успехов)* — событие, связанное с безопасностью системы. Примером такого события является успешная попытка регистрации пользователя в системе.
- *Failure Audit (Аудит отказов)* — событие связано с безопасностью системы. Например, такое событие будет зарегистрировано, если попытка доступа пользователя к сетевому диску закончилась неудачей.

Информация о событиях содержит следующие параметры:

- *Параметр* - Описание
- *Type (Тип)* -Тип события
- *Date (Дата)* - Дата генерации события
- *Time (Время)* - Время регистрации события
- *Source (Источник)* - Источник (имя программы, системного компонента или компонента приложения), который привел к регистрации события
- *Category (Категория)* - Классификация события по источнику, вызвавшему его появление
- *Event ID (Событие)* - Идентификатор события
- *User (Пользователь)* - Учетная запись пользователя, от имени которой производились действия, вызвавшие генерацию события

- *Computer (Компьютер)* - Компьютер, на котором зарегистрировано событие

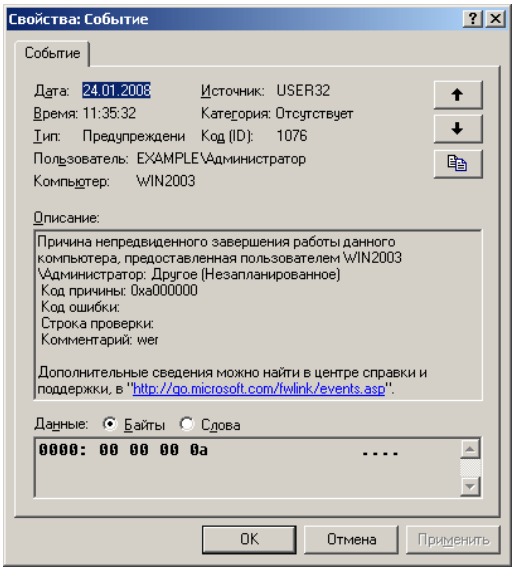


Рисунок. 2. Дополнительная информация о событии.

Выполнение работ

Задание 1. Просмотрите сетевые подключения к компьютеру.

1. Подготовьтесь к выполнению задания:
   - запустите виртуальную машину **VM-2;**
   - создайте на рабочем столе общую папку ***MyFolder*** и разместите в ней документ с именем ***CompName.doc***, содержащий сведения об IP-адресе и символьном имени компьютера;
   - переключитесь в обычный компьютер и откройте документ ***CompName.doc***. Для этого воспользуйтесь **Сетевым окружением**.

Все остальные операции следует выполнять на виртуальном компьютере, где был создан файл ***CompName.doc.***

2. Переключитесь в виртуальную машину **VM-2**.
3. Откройте оснастку **Управление компьютером (*контекстное меню значка Мой компьютер/Управление*)**.
4. Разверните раздел **Общие ресурсы**. *Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.*
5. Отключите общий доступ к созданному ранее ресурсу ***MyFolder***. Для этого в контекстном меню ресурса выберите *Прекратить общий доступ*.
6. Откройте раздел **Сеансы**.
7. Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.
8. Закройте открытый файл. Для этого перейдите в раздел **Открытые файлы** и в контекстном меню файла выберите *Закрыть открытый файл*.

Задание 2 Отключите пользователя с отправкой ему уведомления.

1. Подготовьтесь к выполнению задания. Для этого откройте на обычном компьютере файл ***CompName.doc***, расположенные в виртуальной машине **VM-2**.

2. Переключитесь в виртуальную машину;

3. Откройте оснастку **Управление компьютером**.

4. Выполните для элемента **Общие ресурсы** команду ***контекстного меню/ Все задачи/Отправка сообщения консоли***.

5. Введите в поле **Сообщение** текст выводимого сообщения: *Вы сейчас будете отключены от общего ресурса* и щелкните по кнопке ***Отправить***.

6. Закройте окно **Отправка сообщений консоли**.

7. Для раздела **Открытые файлы** выполните команду контекстного меню ***Отключить все открытые файлы***.

8. Просмотрите пришедшее сообщение.

Задание 3. Просмотрите сведения о процессах системы и ее состоянии.

1. Просмотрите информацию о производительности системы:
   - откройте окно диспетчера задач (**CTRL+SHIFT+ESC**);
   - перейдите на вкладку **Процессы**;

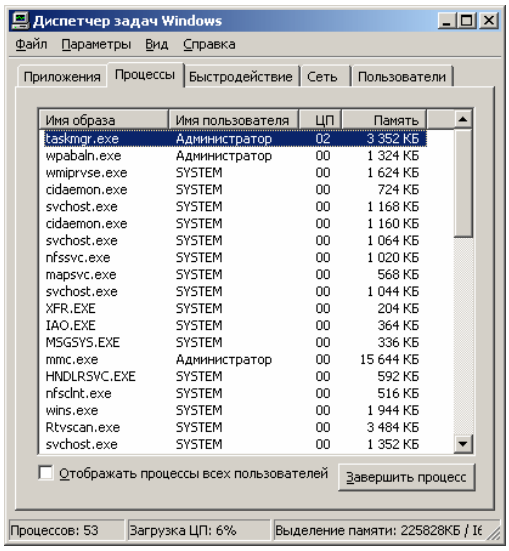


Рисунок 3. Диспетчер задач.

   - просмотрите список и найдите процесс использующий наибольшее количество памяти;
   - перейдите на вкладку **Быстродействие** и посмотрите количество выделенной памяти в соответствующем поле;
   - перейдите на вкладку **Сеть** и ознакомьтесь с информацией о производительности сети;
   - перейдите на вкладку **Пользователи** просмотрите информацию о пользователях, зарегистрированных в системе.

2. Соберите с помощью **Диспетчера задач** информацию, указанную ниже:

Количество запущенных приложений.

Имя процесса, занимающего больше всех оперативной памяти.

Количество выделенной памяти.

Имя пользователя зарегистрированного в системе.

3. Сохраните полученную информацию в личном каталоге в файле формата **ODT**.

Задание 4. Выполните мониторинг сетевых подключений.

1. Запустите оснастку **Производительность**

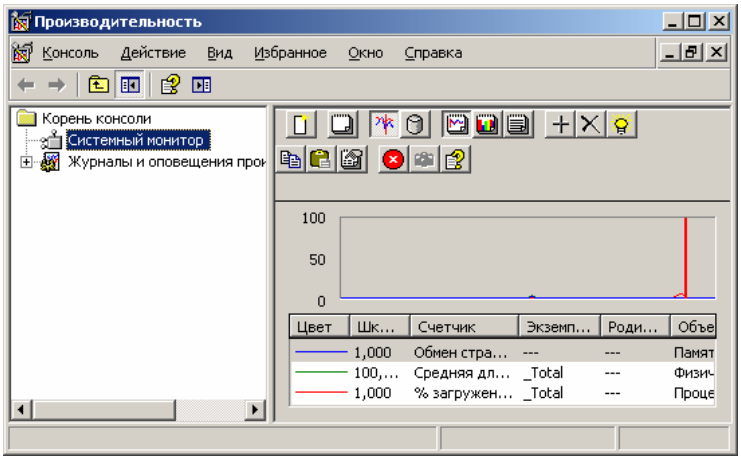


Рисунок 4. Оснастка Производительность

2. Удалите все счетчики из системного монитора:

- активируйте **Системный монитор** в левой части окна **Производительность**;
- откройте диалоговое окно свойств **Системного монитора** кнопкой ***Свойства***  ;
- перейдите на вкладку **Данные**;
- выделите один из счетчиков и удалите его кнопкой ***Удалить***;
- аналогично удалите все остальные счетчики.

3. Добавьте счетчик активных подключений TCP:

- активируйте добавление счетчика кнопкой ***Добавить***;
- выберите в раскрывающемся списке **Объект** – *TCPv4*;
- выберите в списке **Выбрать счетчик из списка** – *Активных подключений*;
- просмотрите информацию о добавляемом счетчике, щелкнув по кнопке ***Объяснение***;
- добавьте счетчик кнопкой ***Добавить***.
- самостоятельно добавьте счетчик ***Всего байт/сек*** для объекта ***Сервер***;
- закройте окно добавления счетчиков кнопкой ***Закрыть***.

4. Закройте диалоговое окно свойств **Системного монитора** кнопкой ***ОК***.

В правой области начнет отображаться информация добавленных счетчиков в графическом виде.

5. Переключите вид отображения информации счетчиков в текстовый вид кнопкой ***Просмотр отчета***  на панели инструментов.

6. Настройте автоматический сбор информации о загруженности сервера в период **с** 8.00 **до** 17.00:

- активируйте раздел **Журналы счетчиков** в левой части окна **Производительность**;
- активируйте создание новых параметров журнала (***Действие/Новые параметры журнала***);
- введите название журнала в поле **Имя** - *Дневная нагрузка* и подтвердите кнопкой ***ОК***;
- добавьте объект **Сервер**:
  - откройте окно добавления объектов кнопкой ***Добавить объект***;
  - выделите в списке **Объект** – *Сервер*;
  - добавьте объект кнопкой ***Добавить***;
  - закройте окно добавления объектов кнопкой ***Закрыть***;
- аналогично добавьте объект **Сетевой интерфейс**;
- установите время сбора данных:
  - перейдите на вкладку **Расписание**;
  - установите в поле **Время** – *8.00*;
  - установите время остановки – *17.00*;
- закройте диалоговое окно параметров нового журнала кнопкой ***ОК***. *В правой части окна* ***Производительность*** *появится новый журнал. Просмотреть результат работы журнала можно в папке* ***C:\perflogs***.

7. Настройте оповещение, если количество доступной памяти станет менее ***100 Мб***.

- активируйте раздел **Оповещения** в левой части оснастки **Производительность**;
- откройте диалоговое окно **Новые параметры оповещения** (***Действия/Новые параметры оповещения***);
- введите **имя новых параметров** - *Мало памяти* и подтвердите ввод кнопкой ***ОК***;

введите в поле **Комментарий** – *Оповещение о малом количестве оперативной памяти*;

- добавьте счетчик ***Доступно МБ*** для объекта **Память**;
- введите в поле **Порог** значение, при котором должно срабатывать оповещение – *100*;

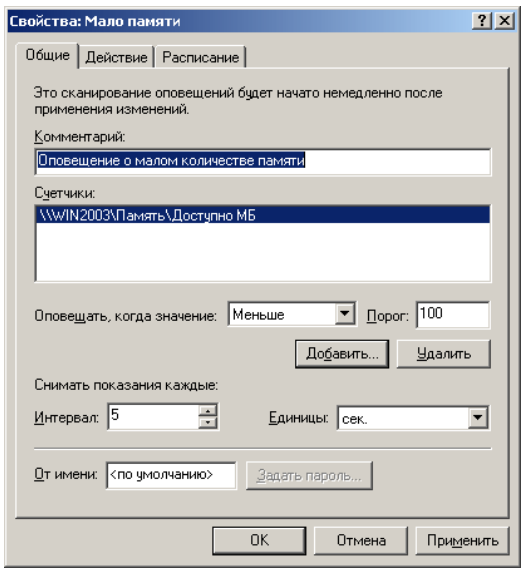


Рисунок 7. Установка параметров оповещения.

- задайте действие, которое должно срабатывать при установленном условии:
  - перейдите на вкладку **Действие**;
  - установите флажок *Послать сетевое сообщение* и введите в поле текст сообщения - *Слишком мало памяти*;
- завершите настройку оповещения кнопкой ***ОК***.

Задание 5. Выполните просмотр событий.

1. Откройте оснастку **Управление компьютером** (***Пуск/Администрирование/Управление компьютером***).
2. Разверните узел **Просмотр событий**.

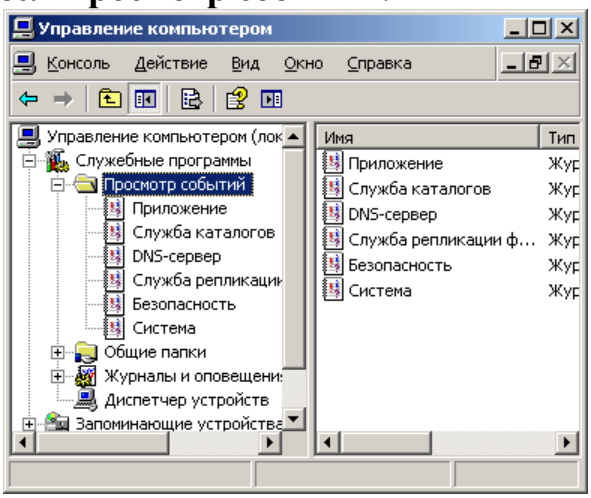


Рисунок 9. Диалоговое окно Просмотр событий.

3. Просмотрите события ***Службы безопасности***:
   - перейдите в раздел **Безопасность** в левой части оснастки **Управление компьютером**;

Справа отобразятся все события данной службы.

- выполните фильтрацию событий только для пользователя ***JustUser***:
  - откройте диалоговое окно свойств раздела **Безопасность** (***Действия/Свойства***);
  - перейдите на вкладку **Фильтр**;

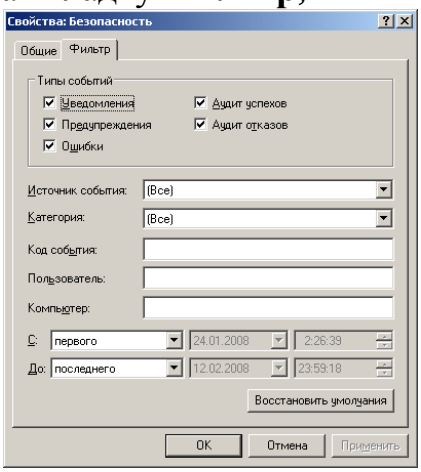


Рисунок 10. Диалоговое окно Фильтр.

  - введите в поле **Пользователь** имя пользователя, для которого необходимо отобразить события, например *JustUser*;
  - самостоятельно установите в полях **С** и **ДО** сегодняшний день;
  - подтвердите применение фильтра кнопкой ***ОК***.
- просмотрите событие ***Доступ к службе каталогов***:
  - найдите указанное событие в правой части окна оснастки **Управление компьютером**;
  - откройте диалоговое **окно свойств** выбранного события (***Действия/Свойства***);
  - ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;
  - закройте диалоговое окно свойств события кнопкой ***ОК***.

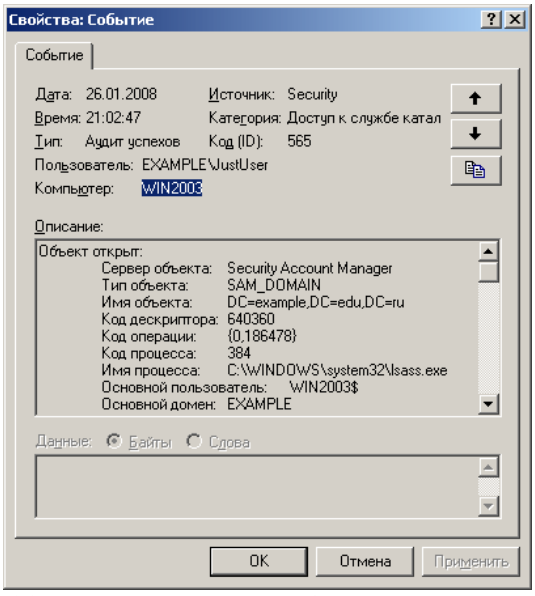


Рисунок 11. Диалоговое окно Свойства события.

- снимите установленный ранее фильтр:
  - откройте диалоговое **окно свойств** раздела **Безопасность**;
  - прейдите на вкладку **Фильтр**;
  - восстановите стандартные значения кнопкой ***Восстановить умолчания***;
  - закройте диалоговое окно свойств раздела **Безопасность** кнопкой ***ОК***.

4. Экспортируйте список событий для раздела **DNS-сервер** в текстовый файл:

- активизируйте раздел **DNS-сервер**;
- откройте **диалоговое окно экспорта** (***Действие/Экспортировать список***);
- введите *имя файла* в поле **Имя**;
- сохраните файл кнопкой ***Сохранить***;
- просмотрите сохраненный файл стандартной программой ***Блокнот***.

Содержание отчета по лабораторной работе

Отчет должен содержать следующую информацию:

- Титульный лист.
- Цель работы.
- Краткое описание и скриншот по каждой из команд.
- Вывод