Предисловие

Этот курс предназначен для системных администраторов сетей на базе Windows 2000 и всех, кто осваивает самую популярную в мире операционную систему фирмы Microsoft. Системный администратор - это специалист, отвечающий за обслуживание серверов и рабочих станций в сети. Для качественного выполнения обязанностей ему необходимы твердые знания в области администрирования Windows 2000 Server и Professional фирмы Microsoft.

Содержание курса

Курс знакомит с основными понятиями, способами и средствами, необходимыми администраторам Windows 2000 для выполнения большинства административных задач. Он разбит на шесть тем, которые, в свою очередь, разделяются на занятия. Как правило, занятия имеют ссылки на практические упражнения, при выполнении которых можно приобрести минимально необходимые практические навыки администрирования. Однако, этот заочный курс не является заменой очных авторизованных курсов Microsoft, но дополняет их. В предлагаемом курсе рассматриваются следующие темы:

1. Семейство операционных систем Windows 2000. Установка Windows 2000.
2. Основные инструменты администратора Windows 2000
3. Протокол TCP/IP: основы адресации

4. Службы DNS и DHCP
5. Структура Active Directory
6. Администрирование Active Directory

Условно можно разделить курс на две части. Первую часть, куда входят темы с 1 по 3, рекомендуется внимательно изучить до обучения на очных авторизованных курсах Microsoft, чтобы изучаемый материал был более знакомым и понятным. Вторая часть, куда входят темы с 4 по 6, предназначен для получения дополнительной информации, которая не будет даваться на очных курсах, либо даваться в ограниченном объеме. По этим причинам рекомендуется изучать вторую часть курса после изучения авторизованного курса Microsoft 2152.

Тема 1

Семейство операционных систем Windows 2000. Установка Windows 2000.

В этой теме:

Рассматриваются особенности и преимущества операционной системы Microsoft Windows 2000. Обсуждаются вопросы подготовки к установке: выбор оборудования, разбиение жесткого диска, варианты обновления, вопросы лицензирования. Пошагово рассматривается процесс установки и особенности выбора настроек.

Занятие 1: "Семейство операционных систем Windows 2000"

Существуют две различные и совершенно самостоятельные "ветви" операционных систем (ОС) Windows:

- для домашних пользователей (Windows 3.x, Windows 9x, Windows Me)
- для бизнеса (Windows NT, Windows 2000, Windows XP)

Windows 2000 - ОС, основанная на технологии Windows NT, что отраженно в первоначальном названии проекта Windows 2000 - Windows NT 5.0. NT (New Technology) была создана группой разработчиков под руководством Дэйва Катлера, ранее работавшего в DEC над проектом VMS (кстати, довольно часто используемая аббревиатура WNT получается из VMS сдвигом букв V, M, S по алфавиту на одну: V->W, M->N, S->T). Дэйв Катлер пришёл в Microsoft в 1988 году специально для работы над проектом NT. Таким образом, NT в некотором смысле проект одного человека, она наиболее законченная ОС из всех выпущенных Microsoft.

Windows 2000 - полностью 32-разрядная ОС с приоритетной многозадачностью и улучшенной реализацией работы с памятью. В основе проекта Windows 2000 лежат те же принципы, которые когда-то обеспечили успех NT:

1. **Совместимость**. Система имеет привычный интерфейс ОС семейства Windows, поддержку файловых систем NTFS5, NTFS4, FAT16 и FAT32. Большинство приложений, написанных под MSDOS, W9x, NT4, а также некоторые программы под OS/2 и POSIX запускаются и функционируют без проблем. При проектировании NT учитывалась возможность работы системы в различных сетевых средах, поэтому в поставку входят средства для работы в Unix- и Novell-сетях.
2. **Переносимость**. Система работает на различных процессорах семейства x86. Реализация поддержки процессоров других архитектур возможна, но не реализована.
3. **Масштабируемость**. В Windows 2000 реализована поддержка технологий SMP и COW (Cluster Of Workstations). Максимально поддерживаемое количество процессоров при использовании SMP - 32.
4. **Система безопасности** полностью удовлетворяет спецификации C2 по терминологии АНБ США. Для полной поддержки C2 требуется оборудование, которое удовлетворяет этой спецификации.
5. **Распределённая обработка**. Windows 2000 имеет встроенную в систему поддержку работы в сети и использование различных протоколов, что обеспечивает возможность связи с различными типами компьютеров.
6. **Надёжность и отказоустойчивость**. Архитектура ОС защищает приложения от повреждения друг другом и самой операционной системой. При этом используется отказоустойчивая структурированная обработка особых ситуаций на всех архитектурных уровнях, которая включает восстанавливаемую файловую систему NTFS и обеспечивает защиту с помощью встроенной системы безопасности и усовершенствованных методов управления памятью.
7. **Локализация.** Система может использоваться во многих странах мира на национальных языках, что достигается применением стандарта ISO Unicode.
8. **Расширяемость.** Благодаря модульному построению системы становится возможно добавление новых модулей на различные архитектурные уровни ОС.

Для России локализованы (переведены на русский язык) следующие версии ОС Windows 2000:

- Windows 2000 Professional, которая применяется на настольных персональных компьютерах (ПК) или на мобильных ПК. Может применяться как клиентская часть для Windows 2000 Server.
- Windows 2000 Server - многофункциональная сетевая операционная система (службы доступа к файлам и принтерам, серверы приложений, контроллеры домена). Это впервые полностью локализованная версия серверной операционной системы фирмы Microsoft.

Возможности операционных систем Windows 2000

Windows 2000 как платформа для внедрения различных веб–решений

- **Internet Information Services 5.0 (IIS)**

  Интегрированный веб–сервер обеспечивает совместный доступ к информации, создание бизнес–приложений для Internet, а также позволяет работать с файлами, принтерами и аудио-/видеоматериалами через Internet.
- **Среда разработки активных страниц сервера Active Server Pages (ASP)**

  Среда Active Server Pages считается самой простой и быстродействующей из существующих сред для написания сценариев на веб–сервере.
- **Использование стандарта XML**

  Создание приложений, позволяющих веб–серверу обмениваться данными в формате XML как с обозревателем Microsoft Internet Explorer, так и с любым компьютером, поддерживающим стандарт XML.
- **Сетевая платформа для мультимедиа служб.**

  С помощью интегрированных служб Windows Media можно формировать потоки высококачественной аудио- и видеоинформации, управлять ими через Internet или в локальной сети, передавая содержимое в режиме реального времени или по запросу.
- **Поддержка работы со службой каталога**

  Разработчики могут использовать несколько стандартных интерфейсов для создания приложений, использующих информацию о пользователях, других приложениях и устройствах, хранимую службой каталогов Active Directory. Все функции службы каталогов Active Directory доступны с помощью протокола LDAP, интерфейсов ADSI и MAPI — для расширения и интеграции с другими приложениями, каталогами и устройствами.
- **Веб–папки**

  Веб–папки позволяют использовать широкие функциональные возможности Windows при работе с документами благодаря протоколу WebDAV (Web Document Authoring and Versioning), позволяющему просто и безопасно публиковать материалы на веб-сайте.
- **Печать через Internet**

  Поддержка протокола IPP (Internet Printing Protocol) позволяет отправлять задания печати на принтер через Internet.

Windows 2000 обеспечивает масштабируемость

и производительность при работе с Internet

- **Службы терминального доступа**

  Выполнение на сервере приложений на основе Windows и доступ с удаленного персонального компьютера, терминала на основе Windows или устройства, где работает отличная от Windows система, по локальным сетям, глобальным сетям или при подключении по линии с низкой пропускной способности путем использования программного обеспечения эмуляции терминала. В системе Windows 2000 уровень масштабируемости служб терминала повышен на 20%. Кроме того, резко повышено быстродействие служб при использовании подключений как с высокой, так и с низкой пропускной способностью.
- **Повышение быстродействия активных страниц сервера (ASP) по сравнению с Windows NT 4.0**

  Дополнительные возможности масштабируемости обработки активных страниц сервера (Active Server Page — ASP), улучшенное управление ASP—потоками и упрощенный способ обработки файлов для ASP–файлов, не содержащих сценариев, позволяет быстрее обрабатывать веб–страницы.
- **Поддержка большего числа узлов по сравнению с Windows NT 4.0**

  Службы Internet Information Services (IIS) 5.0 позволяют поддерживать большее число веб–узлов на одном сервере при сохранении высокого быстродействия.
- **Ограничение загрузки процессора узлом с помощью IIS**

  Можно ограничить время обработки процессором веб–приложения или узла, чтобы обеспечить более высокое быстродействие при обработке других веб–узлов и приложений.

Windows 2000 позволяет безопасно обмениваться данными с сотрудниками, партнерами и заказчиками

- **Поддержка новейших стандартов безопасности**

  Поддерживается защита веб-сайтов с использованием следующих стандартов, например: 56–разрядные и 128–разрядные протоколы SSL и TLS, стандарт безопасности IPSec, Server Gated Cryptography; средства проверки подлинности Digest Authentication и Kerberos v 5 и защиту Fortezza.
- **Интеграция со службой каталогов Active Directory**

  Интеграция службы каталогов Active Directory с инфраструктурой безопасности обеспечивает основу управления безопасностью пользователей, компьютеров и устройств, что облегчает управление системой Windows 2000.
- **Проверка подлинности по протоколу Kerberos**

  Поддержка протокола Kerberos версии 5 повышает уровень безопасности при аутентификации пользователей.
- **Инфраструктура открытых ключей (Public Key Infrastructure — PKI)**

  Сервер сертификатов с открытым ключом на основе сертификатов X.509 дает возможность использовать сертификаты с открытым ключом для проверки подлинности, применения цифровых подписей и обеспечения безопасности связи.
- **Поддержка смарт–карт**

Поддержка входа в систему с помощью смарт–карт, обеспечивающая возможности дополнительной защиты важных для безопасности системы вычислительных блоков, включая проверку подлинности.

- **Шифрование файловой системы**

Шифрование позволяет повысить степень защиты данных на жестком диске. Данные остаются зашифрованными даже при создании резервной копии или архивировании.

- **Безопасные сетевые соединения**

Протокол безопасности IPSec позволяет организовать защищенное соединение для двухстороннего обмена данными по сети предприятия. Служба каталогов Active Directory обеспечивает управление политикой его использования, обеспечивая возможности развертывания в организации любых размеров.

- **Служба маршрутизации и удаленного доступа**

Обеспечивает подключение удаленных сотрудников и филиалов к корпоративной сети с помощью коммутируемых или выделенных линий связи.

- **Поддержка виртуальных частных сетей (VPN)**

Windows 2000 обеспечивает средства безопасного подключения через Internet для удаленных пользователей и удаленных филиалов организации по протоколам PPTP, L2TP или IPSec.

Windows 2000 повышает работоспособность системы

- **Защита системных служб от сбоев**

Windows 2000 не дает возможности некорректно написанным программам вмешиваться в работу системы.

- **Защита файлов Windows**

Предотвращает замещение системных файлов при установке новых приложений.

- **Сертификация драйверов**

Указывает драйвера устройств, прошедшие тест WHQL (Windows Hardware Quality Labs) и предупреждает пользователя при попытке установить несертифицированный драйвер.

- **Защита приложений IIS**

Защита приложений позволяет выполнять веб–приложения в отдельной области памяти от самого веб–сервера, предотвращая возможность сбоя веб–сервера, вызванного выполнением приложения.

Улучшенные возможности серверного и сетевого доступа в Windows 2000

- **Сертификация приложений и защита библиотек DLL**

Приложения, сертифицированные для работы в системе Windows 2000 Server, были протестированы корпорацией Майкрософт для проверки качества и надежности. Обеспечивается защита библиотек DLL, устанавливаемых приложениями, от конфликтов, способных вызвать сбой приложения.

- **Репликация с использованием нескольких основных реплик.**

Для обеспечения возможностей масштабируемости и доступа в распределенных сетях служба каталогов Active Directory поддерживает репликацию с использованием нескольких основных реплик. «Использование нескольких основных реплик» означает, что все реплики в сети равноправны, любую реплику можно изменить и изменения отразятся на всех репликах.

- **Распределенная файловая система (Dfs)**

  Позволяет строить единое иерархическое представление для общих папок на файловых серверах в сети, увеличивая доступность файлов, поскольку поддерживает множественные копии файлов на распределенных серверах.
- **Дисковые квоты**

  Задание квот использования дискового пространства для пользователя и тома позволяет контролировать используемое дисковое пространство и облегчает планирование использования места на диске.

Динамическая настройка системы

- **Динамическое управление томами**

  Добавление новых томов, расширение существующих томов, удаление или добавление зеркала, восстановление дискового массива RAID 5 при работающем сервере без влияния на работу конечного пользователя.
- **Дефрагментация диска**

  Возникающая с течением времени фрагментация может серьезно снизить быстродействие сильно загруженного файлового сервера или веб–сервера. Использование средств дефрагментации улучшают доступность и быстродействие дисков.
- **Загрузка в безопасном режиме**

  Загрузка в безопасном режиме обеспечивает возможность устранения неполадок, возникающих при запуске системы — изменив принятые по умолчанию настройки или удалив вновь установленный драйвер устройства, который был причиной возникновения проблемы.
- **Архивирование и восстановление**

  Возможности архивирования и восстановления облегчают создание архивных копий и последующее восстановление данных в случае отказа жесткого диска. Система Windows 2000 позволяет создавать архивные копии в виде единого файла на жестком диске и ленточных носителях.
- **Автоматический перезапуск**

  Любая служба может быть настроена на автоматический перезапуск в случае сбоя.

Простота развертывания, настройки и использования Windows 2000

- **Программа подготовки системы SysPrep**

  Средство SysPrep позволяет создавать образ жесткого диска компьютера, включающий операционную систему и установленные приложения, который можно скопировать на другие компьютеры, сокращая время развертывания программ.
- **Технология Windows Installer**

  Технология Windows Installer позволяет отслеживать процессы установки приложений и аккуратно выполняет задачи установки и удаления программ.

- **Технология Plug and Play**

  Автоматически обнаруживает и распознает вновь установленные устройства, упрощая настройку сети и уменьшая время на техническое обслуживание
- **Динамическая регистрация в службе DNS**

  Интегрированная с Active Directory и основанная на стандартах Internet, служба DNS (Domain Name System) упрощает присвоение объектам имен и адресов и расширяет возможности масштабирования, производительности и взаимодействия. Объекты, получающие адреса с сервера DHCP (Dynamic Host Configuration Protocol), автоматически регистрируются в службе DNS.
- **Упрощенный поиск принтеров**

  Публикация принтеров в каталоге службы Active Directory позволяет пользователю быстро найти нужный принтер, основываясь на таких критериях, как расположение, поддержка двусторонней печати или скорость печати.

Централизованное управление при снижении общей стоимости владения

- **Служба каталога Active Directory**

  В системе Windows 2000 применена служба Active Directory. Это масштабируемая, соответствующая современным стандартам служба каталогов, которая упрощает управление, повышает безопасность и обеспечивает широкие возможности применения системы Windows 2000 в существующих компьютерных системах. Служба Active Directory осуществляет централизованное управление клиентами и серверами с операционной системой Windows, используя один и тот же интерфейс управления, что уменьшает затраты на управление и поддержку.
- **Средства управления Windows (Windows Management Instrumentation — WMI)**

  Стандартная модель, обеспечивающая единый способ работы с данными управления, полученными из любого источника. Средства WMI обеспечивают эту возможность для программного обеспечения, например, приложений, а расширения WMI для модели драйвера Windows (Windows Driver Model — WDM) обеспечивают ту же возможность для аппаратуры или драйверов устройств. В системе Windows 2000 средства WMI дают возможность управления и другими функциями.
- **Делегирование административных полномочий**

  Служба каталогов Active Directory позволяет администраторам делегировать ряд административных полномочий другим лицам для распределения полномочий управления и улучшения администрирования. Делегирование также помогает крупным организациям с распределенными филиалами уменьшить число поддерживаемых доменов.
- **Единая консоль управления MMC (Microsoft Management Console)**

  Центральная настраиваемая консоль позволяет унифицировать и упростить задачи администрирования сетевых ресурсов. Все функции управления в операционной системе Windows 2000 доступны через консоль управления MMC.
- **Удаленное управление с помощью служб Terminal Services**

  Службы Terminal Services обеспечивают безопасное удаленное администрирование - поддерживается до двух сеансов одновременно, без снижения быстродействия и независимо от выполняемых приложений.
- **Сервер сценариев Windows (WSH)**

Позволяет автоматизировать задачи администрирования сервера с помощью сценариев, вводимых из командной строки, вместо инструментов с графическим пользовательским интерфейсом.

- **Групповая политика**

  Групповая политика позволяет осуществлять одновременное централизованное управление группами пользователей, компьютеров, приложений и сетевых ресурсов. При этом интеграция со службой Active Directory позволяет достигнуть высокой гибкости и избирательности управления.
- **Централизованное управление настройками рабочей среды пользователей**

  Используя групповые политики, можно управлять настройками рабочей среды пользователей. Технологии управления IntelliMirror позволяют устанавливать и настраивать программы, задавать настройки для компьютеров и пользователей и обеспечивать постоянный доступ к данным пользователей.
- **Средства настройки безопасности**

  Упрощают настройку и анализ безопасности в сетях на базе Windows. В системе Windows 2000 настройки безопасности входят в состав групповой политики.
- **Средства миграции доменов Windows NT 4.0**

  Упрощают процесс обновления до домена Windows 2000.

Сохранение существующих инвестиций в ИТ–инфраструктуру при внедрении Windows 2000

- **Широкие возможности совместной работы с клиентскими компьютерами**

  Поддерживает операционные системы Windows NT Workstation, Windows 9x, Windows 3.x, Macintosh и Unix.
- **Взаимодействие служб каталогов и приложений**

  Служба каталогов Active Directory может взаимодействовать и синхронизировать данные с другими службами каталогов, используя протокол LDAP (Lightweight Directory Access Protocol), синхронизацию через службу MSDSS (Microsoft Directory Service Synchronization) или средство ADC (Active Directory Connector).
- **Службы Services for NetWare**

  Дополнительный продукт, обеспечивающий возможности взаимодействия серверов и клиентов NetWare с серверами и клиентами Windows.
- **Службы Services for Unix**

  Дополнительный продукт, упрощающий встраивание операционных систем Windows NT 4.0 и Windows 2000 в среду UNIX

Занятие 2: "Требования к аппаратным и системным ресурсам"

Прежде чем устанавливать систему Windows 2000, нужно точно знать, соответствуют ли аппаратные ресурсы данной ОС.

Для этого нужно обратиться к списку совместимых аппаратных ресурсов **HCL**(Hardware Compatibility List). Копия списка HCL находится в файле **Hcl.txt** в папке **Support**, расположенной на дистрибутивном компакт-диске Windows 2000. Последнюю версию списка HCL можно увидеть на веб-узле Microsoft по адресу: http://www.microsoft.com/htwtest/hcl

Корпорация Майкрософт поставляет проверенные драйверы только для устройств, включённых в список HCL. HCL - это перечень аппаратных устройств, официально тестировавшихся на совместимость с Windows 2000. Использование оборудования, не входящего в список HCL, может вызвать неполадки во время установки, и после её завершения.

Системные требования для ОС Windows 2000 (без установки каких-либо приложений пользователя)

Компонент	**Windows 2000 Professional**	**Windows 2000 Server**
Процессор	Pentium 133 МГц или выше. До двух процессоров	Pentium 133 МГц или выше. До четырёх процессоров
Память	Минимум - 32 Мбайта, рекомендуется не менее 64 Мбайт	Минимум - 64 Мбайта, рекомендуется не менее 256 Мбайт
Пространство на жёстком диске	2 Гбайта, с объёмом свободного пространства не менее 1 Гбайта	2 Гбайта, с объёмом свободного пространства не менее 1 Гбайта
Монитор	VGA или с более высоким разрешением	VGA или с более высоким разрешением
Дополнительное оборудование	Клавиатура и мышь	Клавиатура и мышь
Для установки с компакт-диска	12-скоростной или более быстрый дисковод	12-скоростной или более быстрый дисковод

Занятие 3: "Подготовка к установке Windows 2000"

Перед установкой операционной системы Windows 2000 необходимо выполнить следующее:

1. Проверить соответствие компонентов аппаратных средств минимальным требованиям.
2. Убедиться в наличии драйверов для оборудования, совместимых с Windows 2000.
3. Определить, требуется ли произвести обновление или выполнить новую установку.
4. Запланировать разбиение жесткого диска на разделы и используемую файловую систему.
5. Иметь серийный номер продукта. При установке сервера - знать количество купленных лицензий и режим лицензирования.
6. Знать структуру сети и продумать настройку протоколов и адресов.

Драйвера для оборудования.

Перед установкой любой операционной системы нужно убедиться в том, что аппаратные компоненты компьютера будут поддерживаться операционной системой. Программа установки системы Windows 2000 поддерживает режим отчета, в котором можно генерировать отчеты о совместимости. Эти отчеты содержат информацию о несовместимых элементах и приложениях, которая будет полезна перед проведением обновления. Проанализировав такой отчет, можно определить, следует ли устанавливать пакеты обновления или новые версии приложений.

Отчет о совместимости можно сгенерировать двумя способами:

- Если на компьютере уже установлена 32-х битная ОС Microsoft, то можно выполнить команду **winnt32 /checkupgradeonly** Эта команда запускает первый этап программы установки системы Windows 2000. Вместо того, чтобы выполнять всю программу установки целиком, данная команда только проверяет оборудование и программное обеспечение на совместимость, а затем составляет отчет о совместимости.
- Запустить программу Windows 2000 Readiness Analyzer (Анализатор готовности Windows 2000). Она проверяет, можно ли обновить компьютеры, работающие под управлением системы Windows 95, Windows 98 или Windows NT, до уровня Windows 2000. Эта программа выявляет устройства и приложения, несовместимые с системой Windows 2000.

  Указанная программа доступна по адресу
  http://www.microsoft.com/windows2000/upgrade/compat/default.asp

Если в отчете о совместимости указано, что какое-то оборудование несовместимо с Windows 2000, не стоит паниковать раньше времени. Поскольку с момента выхода Windows 2000 прошло уже около 3 лет, эти данные могли устареть. Чтобы точно проверить эту информацию, необходимо зайти на сайт производителя и выяснить, есть ли для данного оборудования драйвера под Windows 2000. По этой причине рекомендуется скачать обновленные драйвера от производителей для всего оборудования, установленного в компьютере, поскольку, скорее всего, Windows 2000 будет устанавливать устаревшие драйвера.

Обновление или установка с "нуля"?

При обновлении операционной системы до Windows 2000 большое значение имеет, с какой операционной системы производится обновление.

Системы Windows NT Workstation 3.51, Windows NT Workstation 4.0 и Windows 2000 Professional

используют общий реестр, общую файловую систему, общую систему безопасности и общие структуры ядра операционной системы, поэтому практически все приложения, работающие в среде Windows NT Workstation 4.0, смогут без изменений работать и в системе Windows 2000 Professional. Обновить систему Windows NT Workstation до уровня Windows 2000 Professional легче, чем любую другую операционную систему Windows, по следующим причинам:

- Почти все периферийное оборудование и устройства, работавшие в среде Windows NT Workstation 4.0, будут работать и в системе Windows 2000 Professional.
- В процессе обновления версия файловой системы NTFS, используемая в системе Windows NT Workstation 4.0, прозрачным образом обновляется до версии NTFS, применяемой в системе Windows 2000 Professional.

Для обновления систем Windows 95 и Windows 98 может потребоваться больший объем работ по планированию и тестированию, чем для обновления системы Windows NT. Из-за различий в системном реестре и процедурах установки многие приложения устанавливаются на компьютерах, работающих под управлением системы Windows 95 или Windows 98, иначе, чем на компьютерах, работающих под управлением системы Windows NT Workstation 4.0 или Windows 2000 Professional. Используйте варианты, указанные в предыдущем разделе, чтобы создать отчеты о совместимости и понять, можно ли вообще установить на этот компьютер Windows 2000. При несовместимости приложения с Windows 2000 попробуйте найти новую версию этого приложения или переустановите Windows 2000 с "нуля" (тогда нужно заменить существующую программу на аналогичную, но работающаю под Windows 2000).

Установку с "нуля" также стоит выполнять, если не требуется сохранять весь набор установленных приложений и их настроек.

Разбиение жесткого диска на разделы и выбор используемой файловой системы.

При разбиении диска на разделы физический диск подразделяется на фрагменты, каждый из которых функционирует независимо. При создании разделов на диске выделяется одна или несколько областей, которые могут быть отформатированы для использования различными файловыми системами, такими как FAT (File Allocation Table - таблица размещения файлов) или NTFS (NT File System - файловая система Windows NT).

NTFS

В системе Windows 2000 рекомендуется использовать файловую систему NTFS. Эта файловая система поддерживает для своих разделов следующие возможности.

- Безопасность на уровне файлов и на уровне папок. Файловая система NTFS позволяет управлять доступом к файлам и папкам.
- Сжатие файлов. Файловая система NTFS сжимает файлы для высвобождения места на диске.
- Дисковые квоты. Файловая система NTFS позволяет контролировать использование диска каждым пользователем.
- Шифрование файлов. Файловая система NTFS обеспечивает прозрачное шифрование содержимого файлов.

Windows 2000 и Windows NT - единственные операционные системы, которые могут работать с данными на локальном жестком диске, имеющем формат NTFS.

FAT и FAT32

Раздел, предназначенный для размещения системы Windows 2000, рекомендуется форматировать с помощью файловой системы FAT или FAT32 только в тех случаях, если используется конфигурация с двумя операционными системами.

Файловая система FAT не поддерживает разделы размером свыше 2 ГБ. Если попытаться отформатировать в файловой системе FAT раздел объемом более 2 ГБ, программа установки автоматически отформатирует этот раздел в файловой системе FAT32.

Вопросы лицензирования.

Программное обеспечение защищено законами об авторских правах. Лицензионное соглашение определяет, как и на каких условиях клиент может использовать программный продукт. До начала установки продукта клиент обязан ознакомиться с условиями лицензионного соглашения. Если клиент не согласен с условиями соглашения, он должен вернуть продукт поставщику.

Серверные продукты предполагают несколько вариантов схемы лицензирования. Так, Windows 2000 Server может лицензироваться по числу одновременных подключений к одному серверу (Per Server) или на число работающих в сети пользователей (Per Seat). Поскольку из режима Per Seat уже переключиться обратно нельзя, рекомендуется выбирать режим лицензирования Per Server. При этом нужно учесть, что приобретённое вами количество лицензий для сервера позволит одновременно подключиться к серверу только этому количеству клиентов (рабочих станций).

Существуют также специальные версии продуктов, предназначенные для поставки только вместе с компьютерным оборудованием, называются OEM (Original Equipment Manufacturer)-версиями продуктов. В момент продажи компьютерного оборудования с предустановленной версией сертификат наклеивается на корпус оборудования, подтверждая тем самым установку лицензионной версии продукта. Этим действием лицензия жёстко закрепляется за конкретным оборудованием.

Посмотреть последние данные о лицензионной политике компании Майкрософт всегда можно на локализованном веб-сайте, по адресу: http://www.microsoft.com/rus/licensing

Настройка протоколов и адресов.

При установке Windows 2000 Server крайне важно запланировать, какие протоколы и адреса будут использоваться сервером. Для этого необходимо иметь представление о уже существующей сетевой инфраструктуре. Прежде всего, это связано с тем, что серверу необходимо присвоить статический IP адрес, по которому будут обращаться пользователи. Более подробно о IP-адресах см. тему 3.

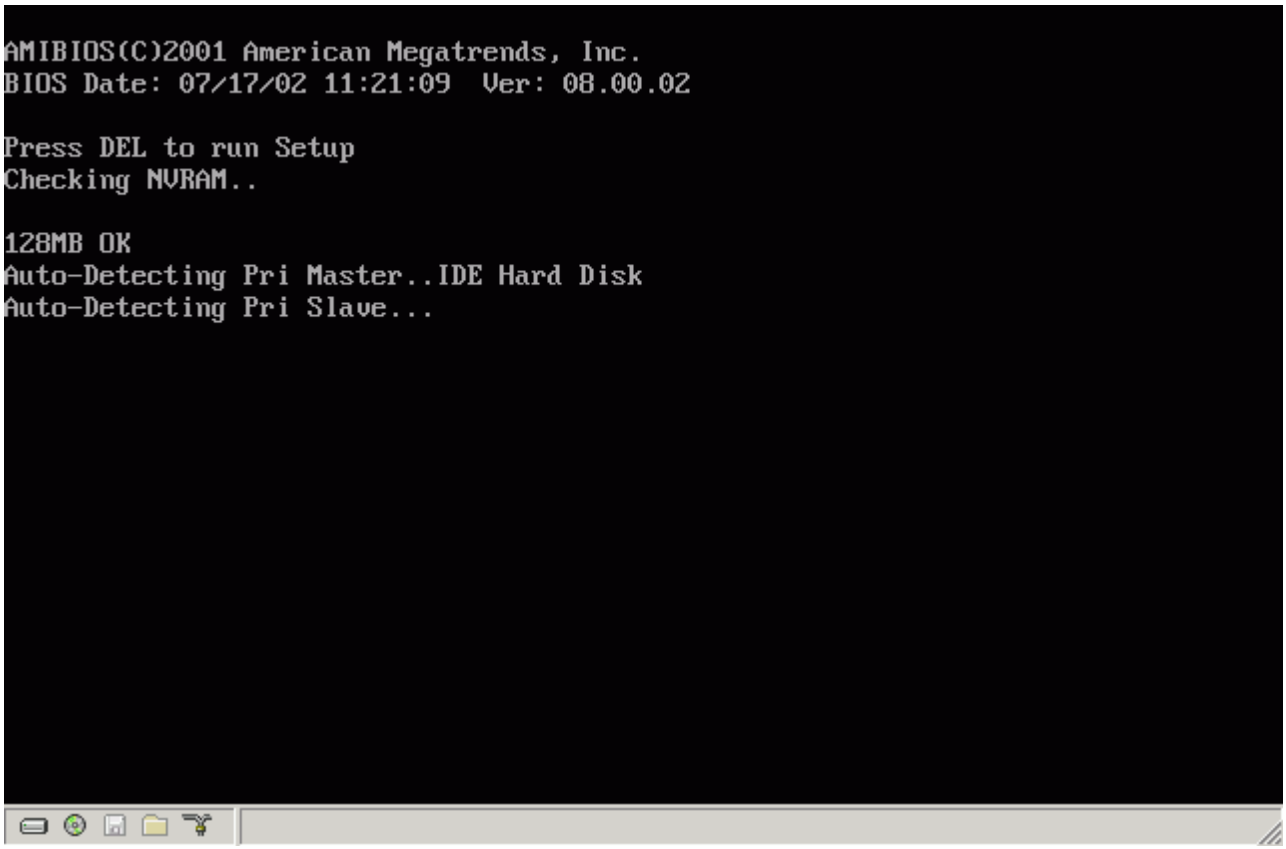
При установке Windows 2000 Professional обычно не важно, какой конкретно адрес будет использоваться этой рабочей станцией, поэтому чаще всего в сети настраивают службу DHCP, которая автоматически выдает динамические IP-адреса, а при установке Windows 2000 по умолчанию уже настроена на получение IP-адреса от DHCP сервера. Более подробно о службе DHCP см. тему 4.

Занятие 4: "Процедура установки Windows 2000 Professional"

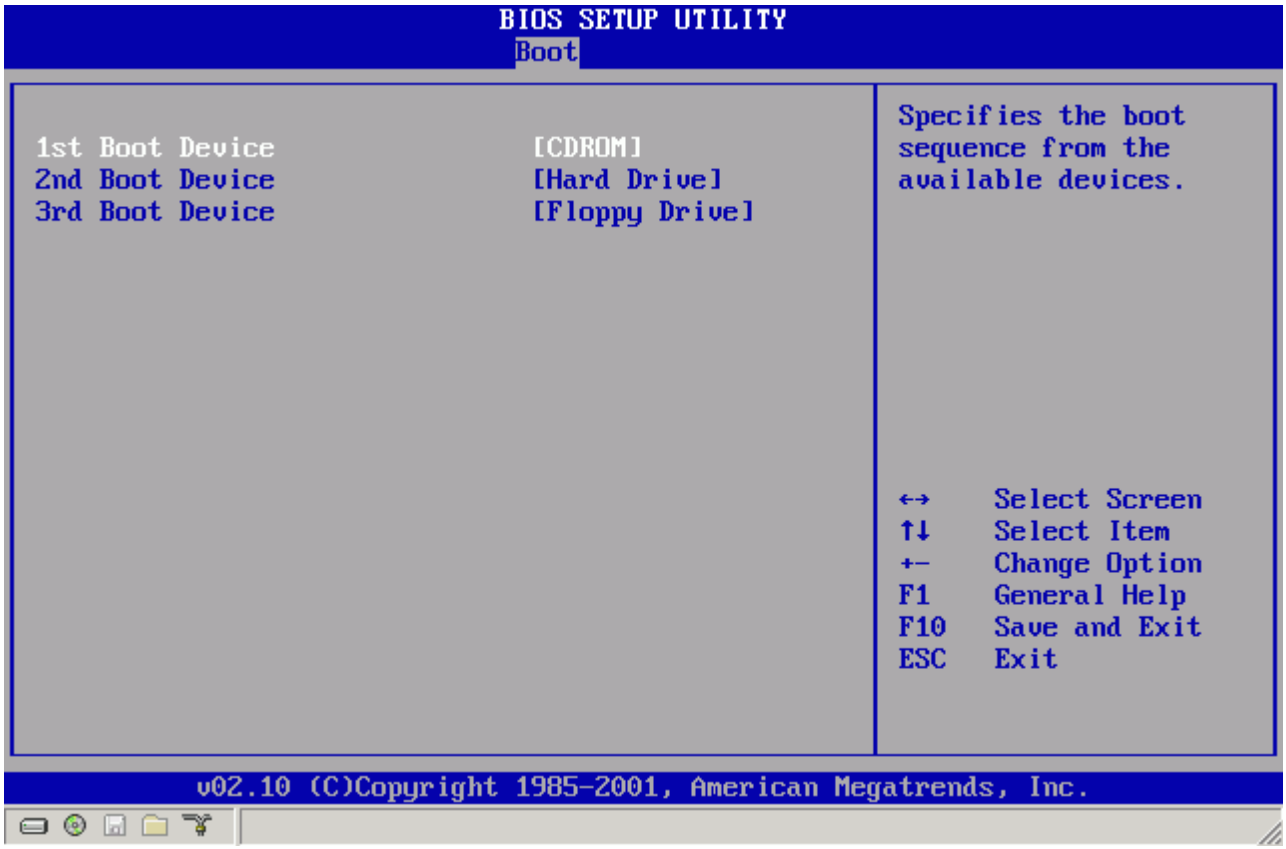
Настройки BIOS

При установке Windows 2000 Professional с компакт-диска, необходимо проверить перед началом установки в "Программе настройки компьютера" (BIOS SETUP) порядок загрузки подключённых периферийных устройств (загрузка должна начинаться с компакт-диска) и правильность установки системных даты и времени.

Для этого включите компьютер. При появлении на экране монитора надписи "Press **DEL** to run Setup" (может быть клавиша **F10** или **F2**, - смотрите документацию на системную плату), нажмите указанную клавишу.



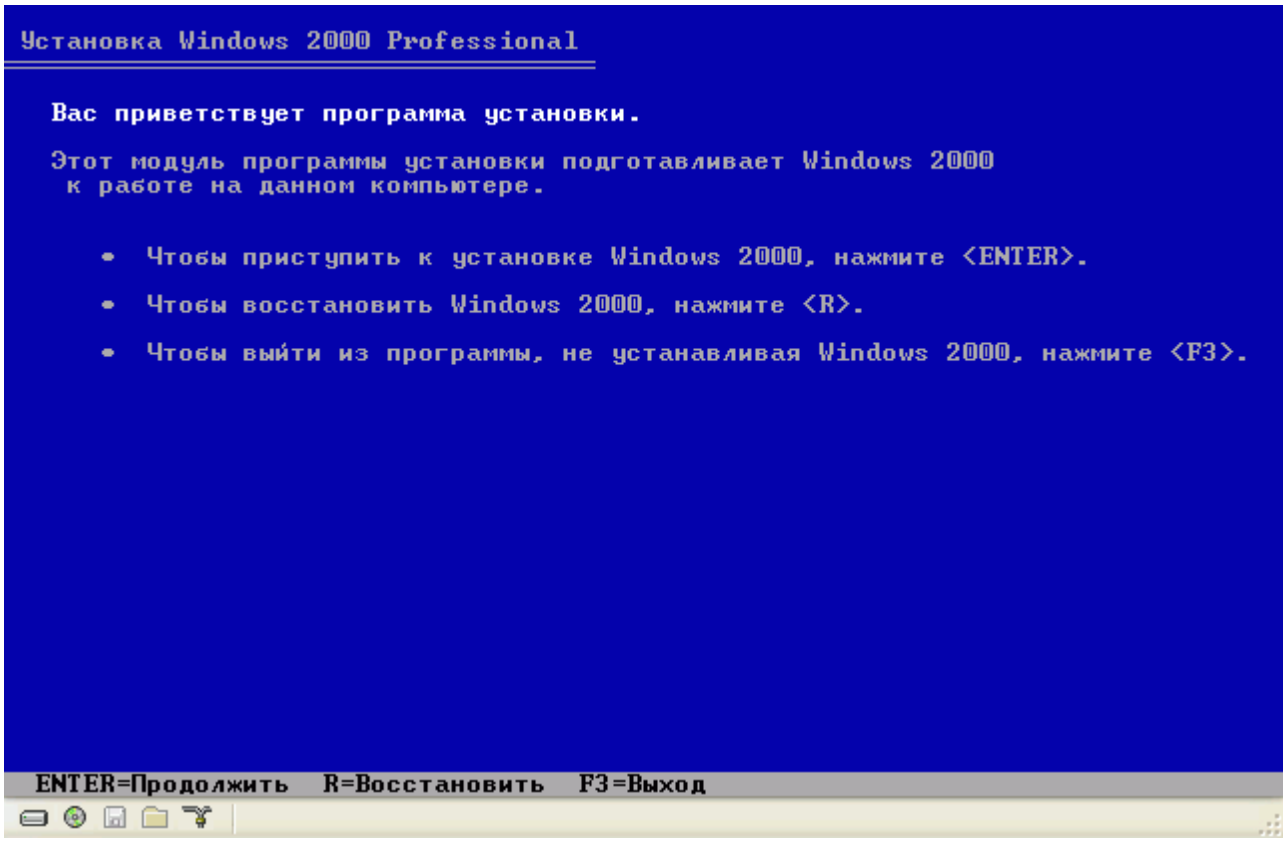
В появившемся на экране меню выберите пункт "BOOT" (в некоторых BIOS'ах эти настройки не выделены в отдельный пункт, а находятся на закладке "BIOS FEATURES (или ADVANCED) SETUP"), нажмите **Enter**. Проверьте последовательность загрузки (этот пункт может называться, например, "Boot sequence"). Первым устройством, с которого начинается загрузка, должен быть установлен накопитель CD-ROM.



Нажмите **ESC**, в появившемся на экране меню выберите пункт "SAVE ?**Y** для перезагрузки компьютера.

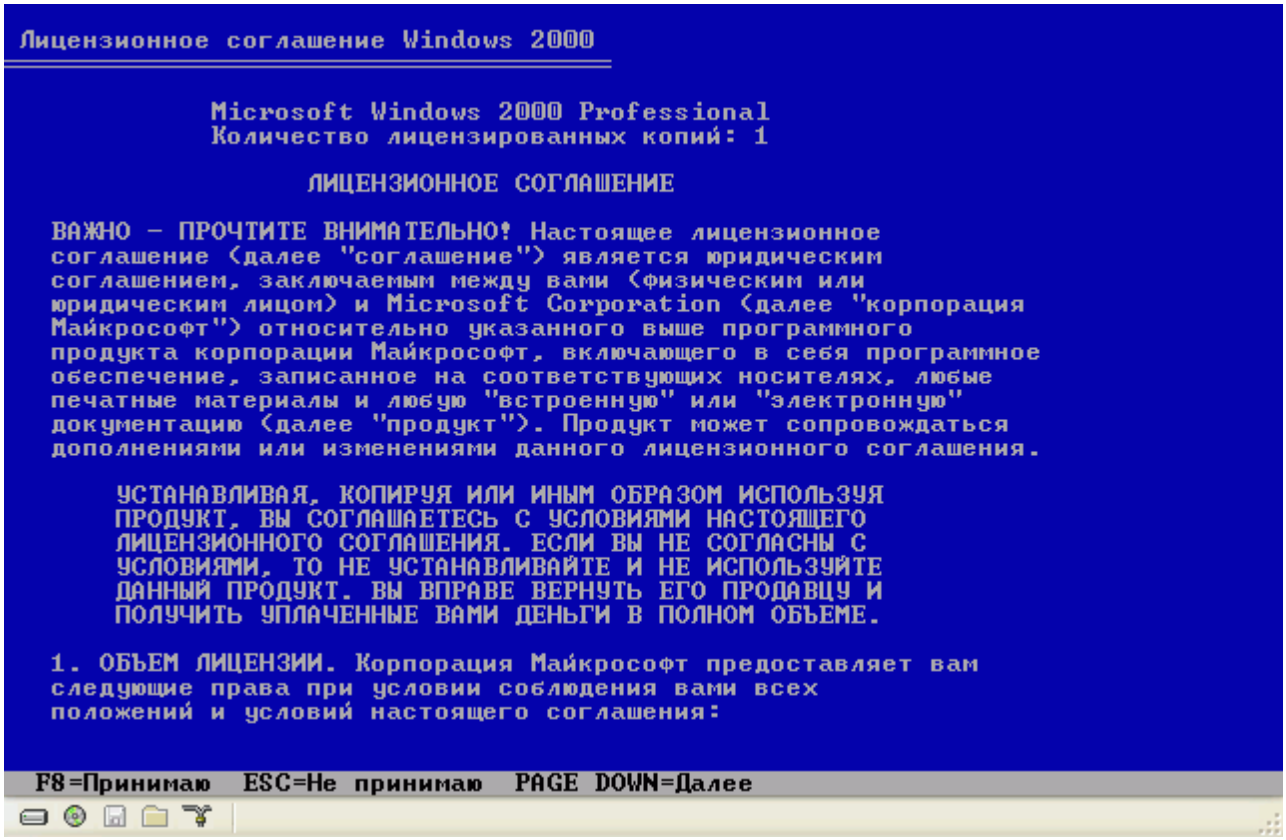
Начало установки

После перезагрузки дождитесь приглашения "Press any key to boot from CD..." и нажмите любую клавишу, чтобы запустить процедуру установки. Нажмите **ENTER**, чтобы продолжить установку или **R** , чтобы начать процедуру восстановления поврежденной Windows 2000.



Лицензионное соглашение

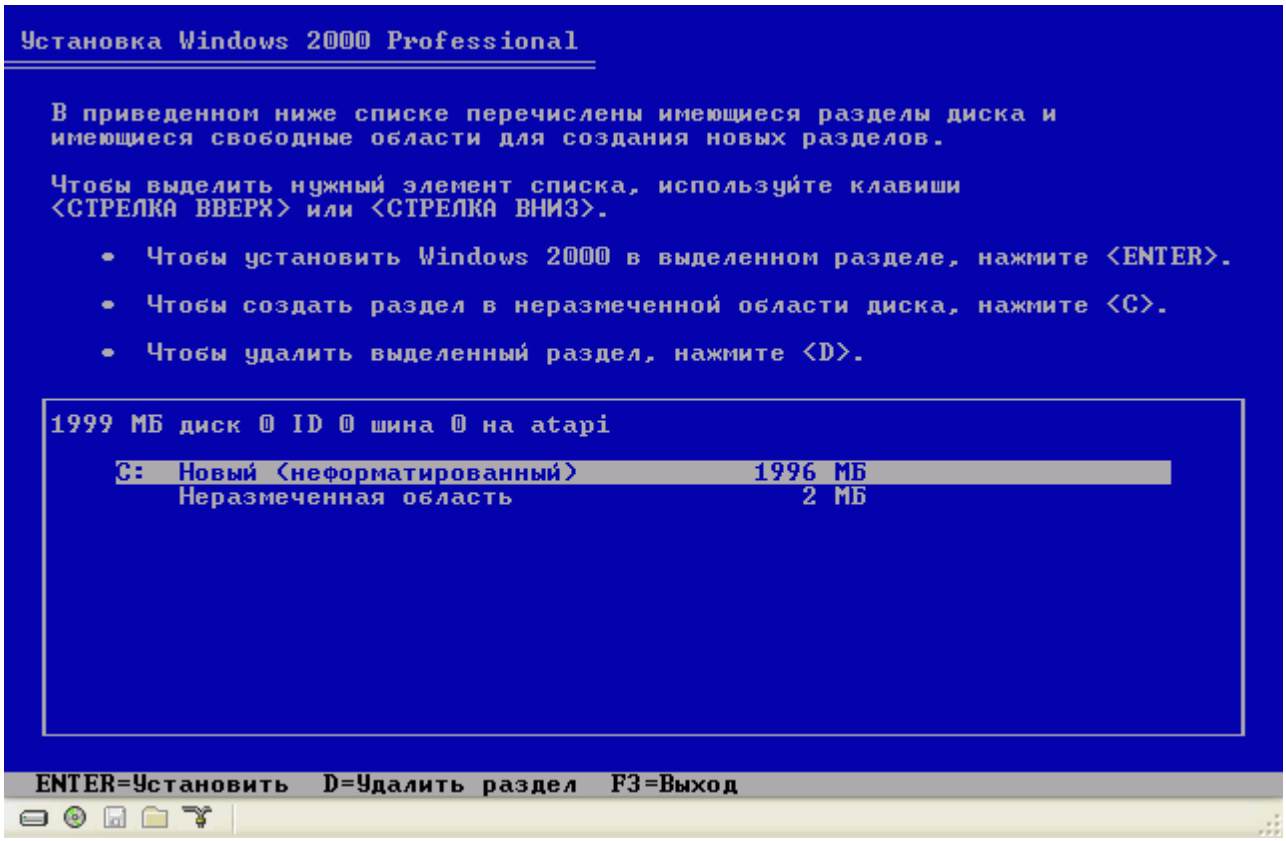
Внимательно прочтите лицензионное соглашение и нажмите **F8**, чтобы согласиться и продолжить установку.



Выбор варианта разбиения диска

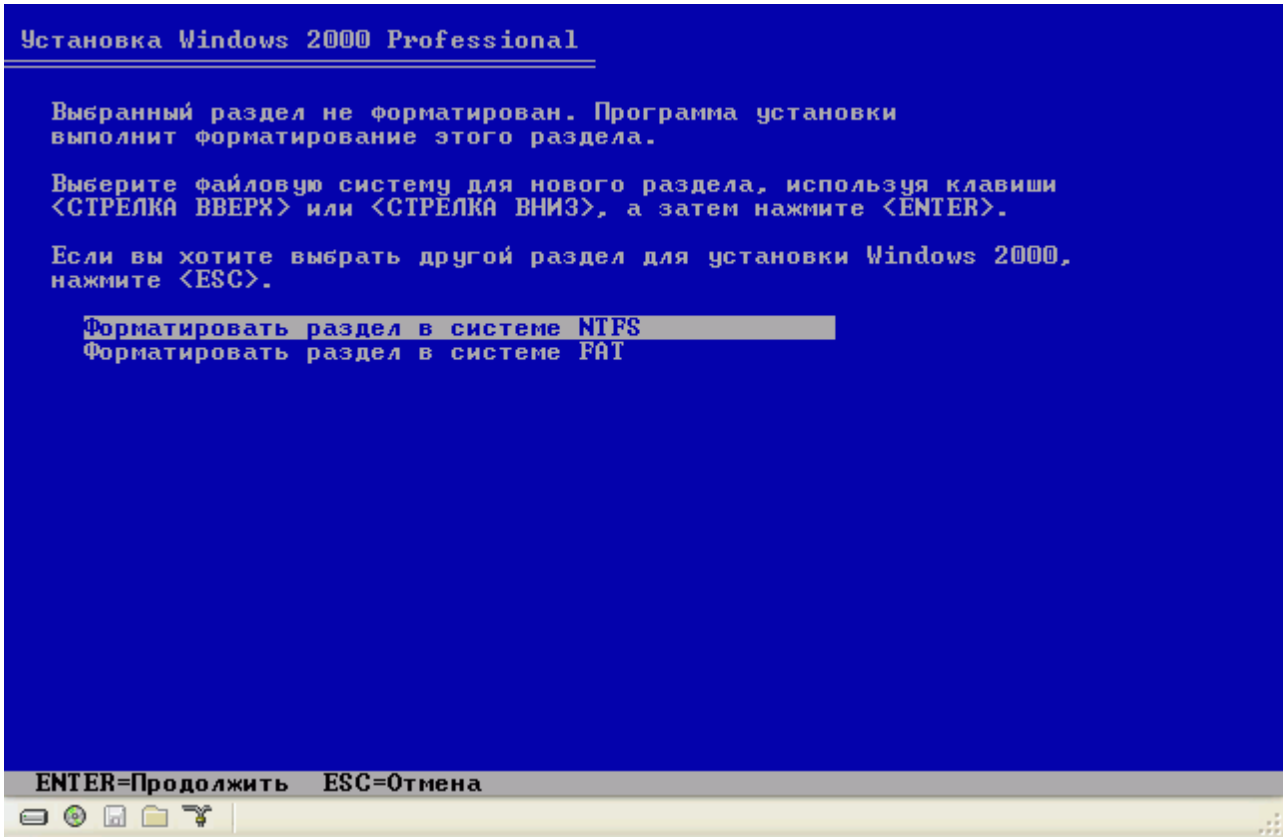
При запуске процедуры установки на новом компьютере с компакт-диска программа установки изучает жёсткий диск и определяет его текущую конфигурацию. Для установки Windows 2000 Server рекомендуется создать новый раздел не менее 4 Гбайт на неразмеченном жестком диске, при установке Windows 2000 Professional для системы вполне достаточным будет раздел в 2 Гбайта. Рекомендуется создавать отдельный раздел, предназначенный только для системы Windows 2000 (не бойтесь оставлять неразмеченную область на диске, её можно быстро использовать при необходимости). После установки системы Windows 2000 оставшуюся часть жёсткого диска можно разметить с помощью инструмента "Управление дисками" - инструмента, предназначенного для управления жёсткими дисками и томами на них.

Примечание. Если установлены две операционные системы, можно при каждом запуске компьютера выбирать, какую из двух систем следует загрузить. При запуске появляется экран, отображаемый в течение определенного числа секунд; на нем предлагается выбрать одну из установленных операционных систем.

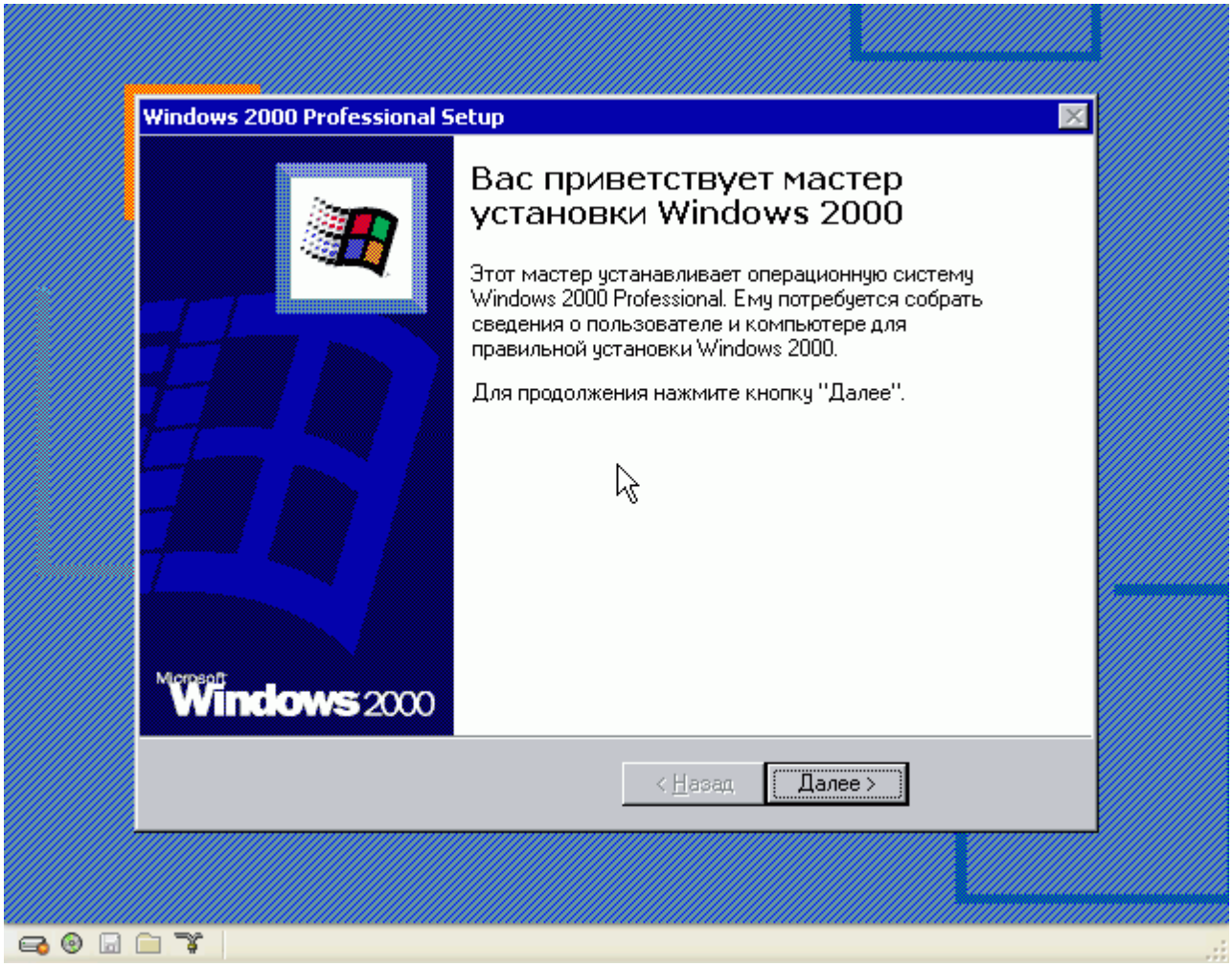


Выбор файловой системы

На компьютере с Windows 2000 Server для разделов диска имеется возможность выбора файловой системы: NTFS или FAT. Если на компьютере уже установлены другие операционные системы, и необходимо их сохранить, либо нужно иметь доступ к диску с этих операционных систем, единственный выбор - FAT. Во всех остальных случаях рекомендуется выбирать файловую систему NTFS. Более подробно о выборе файловой системы см. [занятие 3](#).



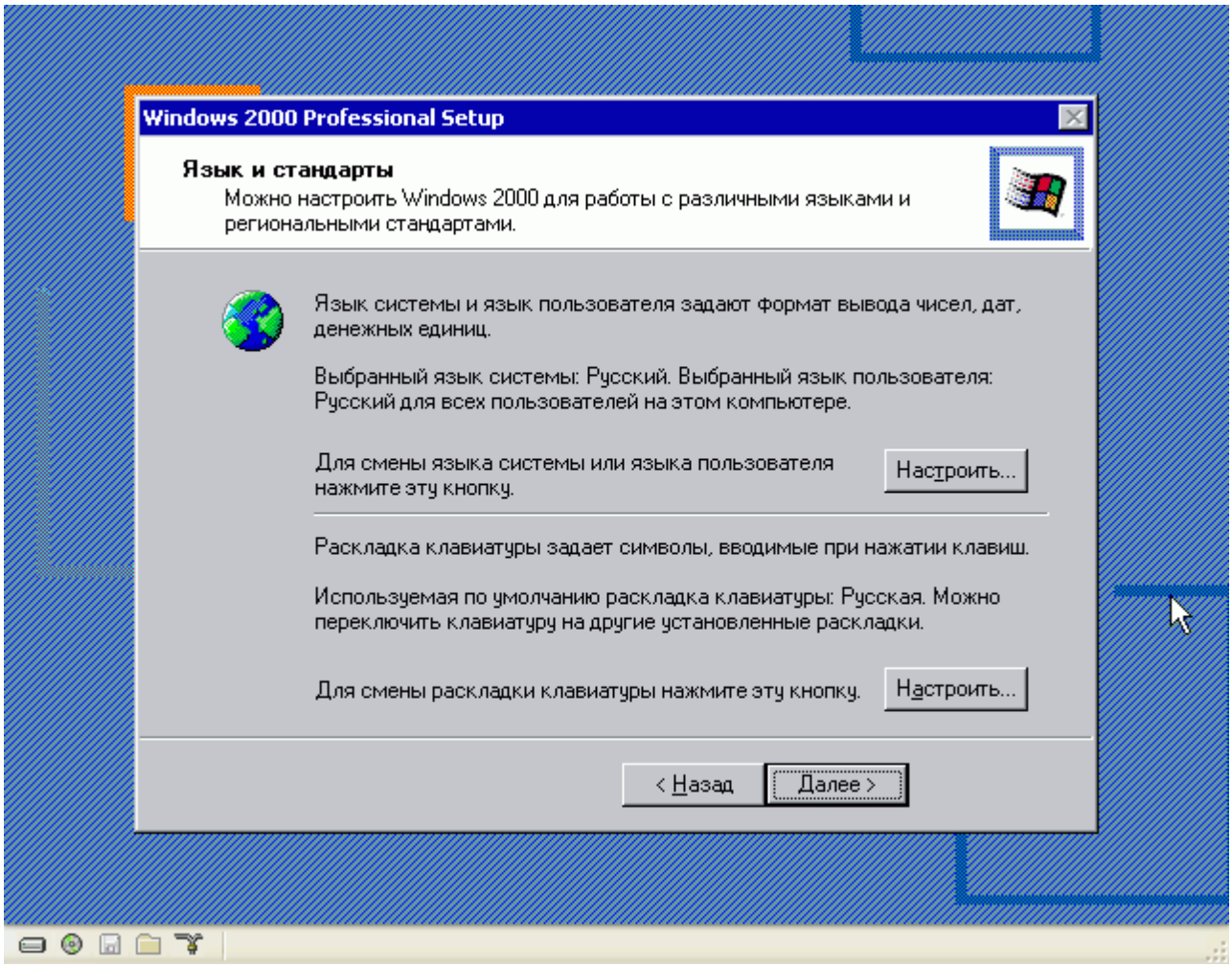
После завершения форматирования выбранного раздела и копирования файлов программы установки на жесткий диск, система автоматически перезагрузится и продолжит установку в графическом режиме.



Настройка системы с учётом национальной специфики

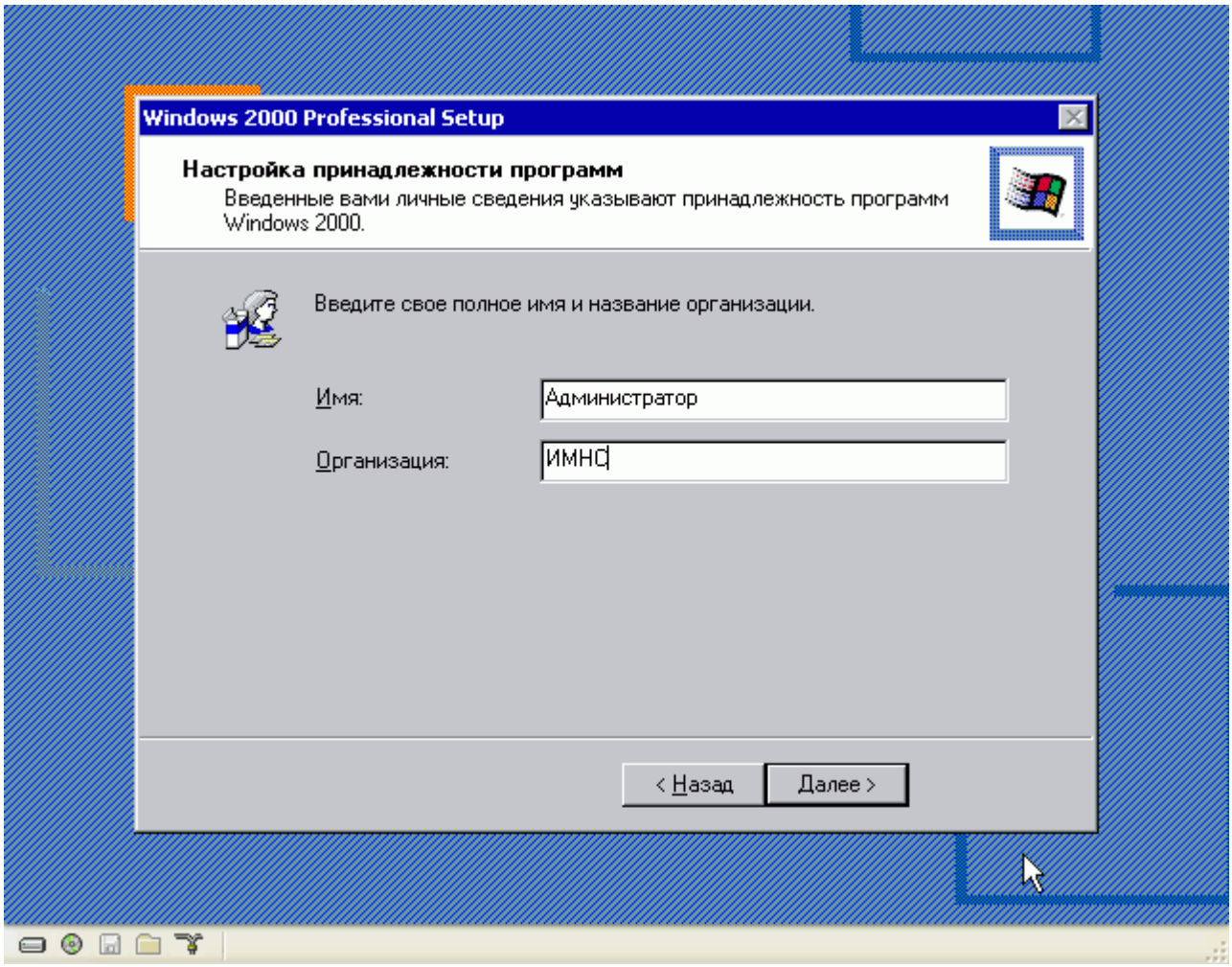
Что такое национальная специфика? Это совокупность принятых в стране требований к языку, формату представления времени, чисел, название дней недели и месяцев года, сведения о кодировании символов и так далее. Например, в русском языке 33 буквы, нет деления времени на до и после полудня, денежная единица - рубль. Windows 2000 имеет язык системы (в нашем случае - русский) по умолчанию и один или несколько языков ввода (чаще всего это английский, дополнительно могут быть по выбору и другие языки). Для добавления или изменения языка после установки Windows 2000 следует воспользоваться инструментом **Язык и стандарты** из **Панели управления**. Windows 2000 использует 16-битную кодировку Unicode в качестве основной кодировки символов, а также поддерживаются кодовые страницы OEM (для MS-DOS) и ANSI (8-битная кодировка).

Единственные изменения, которые стоит сделать здесь при установке русской версии Windows 2000 Professional - добавить в настройках раскладки клавиатуры английский язык.



Персонализация

В этом окне вводится информация о пользователе, которому принадлежит устанавливаемая рабочая станция. Введенные здесь данные будут в дальнейшем использоваться всеми программами, устанавливаемыми на данный компьютер.

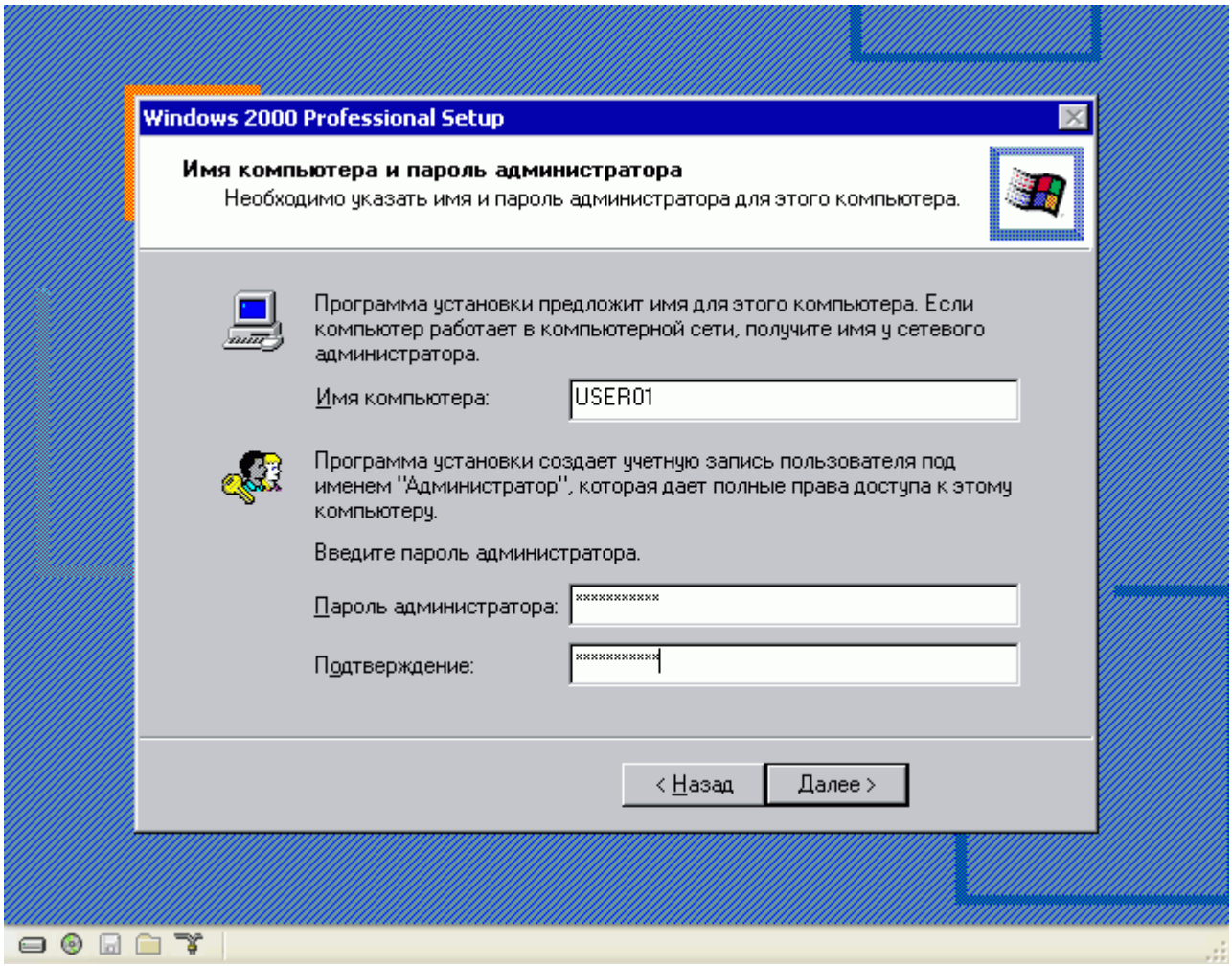


Установка имени компьютера и пароля администратора

Рекомендуемая длина имени компьютера — не более 15 символов, причем рекомендуется использовать только стандартные символы Интернета: числа от 0 до 9, латинские заглавные и строчные буквы от A до Z и символ переноса (-). Использование нестандартных символов может затруднить использование в сети программного обеспечения третьих фирм. Кроме того, если компьютер планируется подключить к домену, следует указать его имя, отличное от всех остальных имен компьютеров, входящих в этот домен.

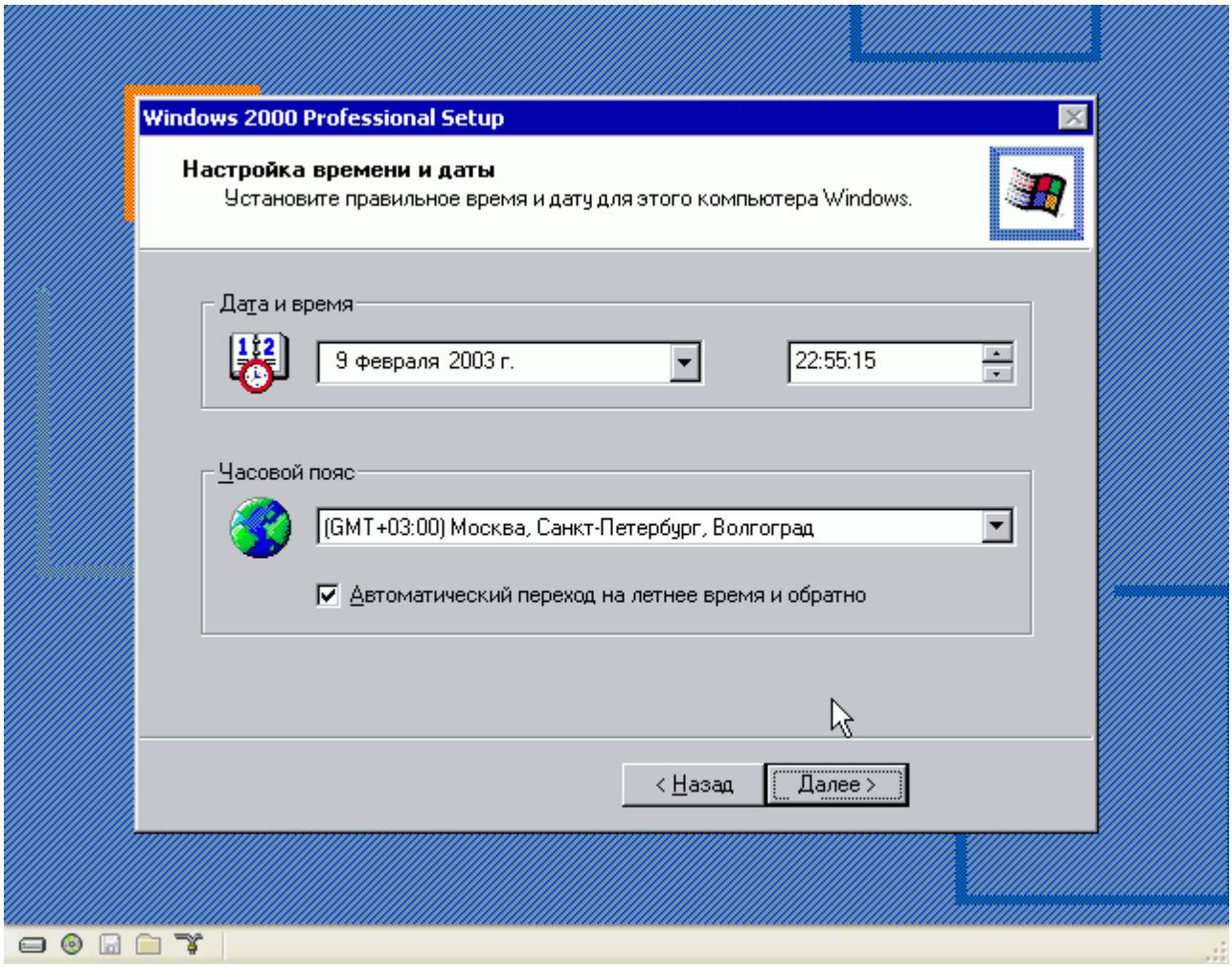
Программой установки Windows 2000 на компьютере создается учетная запись пользователя, называемого администратором и имеющего все права на полное управление конфигурацией компьютера. Учетная запись администратора локального компьютера присваивается пользователю, производящему установку. В целях безопасности учетную запись администратора рекомендуется всегда защищать паролем, причем его длина должна составлять не менее 8 символов. Пустое поле **Пароль администратора** означает его отсутствие для данной учетной записи. Рекомендуется по окончании установки системы в целях повышения безопасности переименовать учетную запись администратора (удалить ее невозможно).

Пароль, введенный в поле **Подтверждение**, должен в точности соответствовать паролю, введенному в поле **Пароль администратора**. Обязательно запомните этот пароль и соблюдайте меры по его защите. Также следует помнить, что пароль чувствителен к регистру прописных/строчных букв.



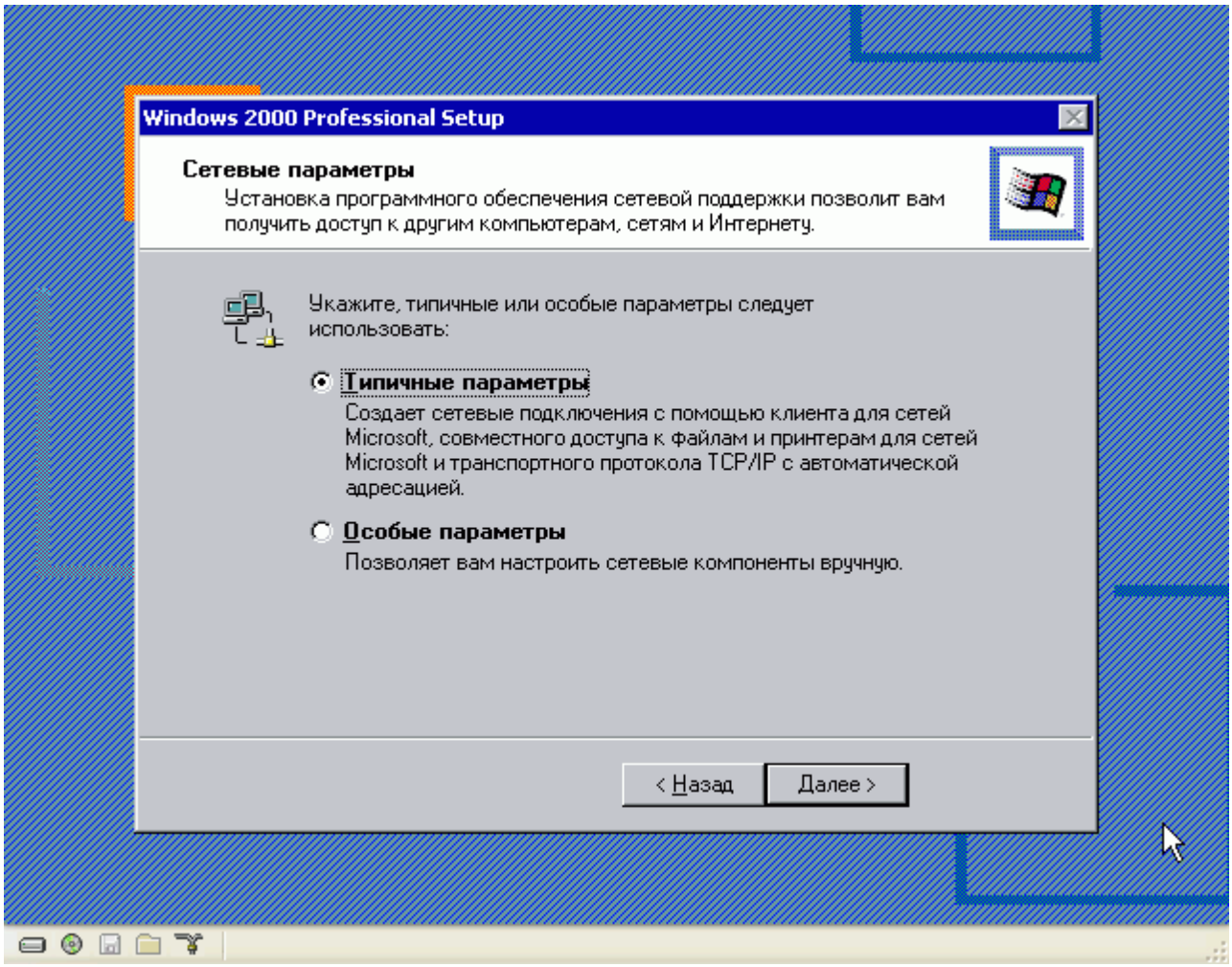
Настройка даты и времени

Проверьте точность установленных даты и времени, а также установленный часовой пояс. Если параметры даты или времени будут отличаться от аналогичных параметров на серверах контроллерах домена более чем на 5 минут (параметр по умолчанию), это может вызвать проблемы при работе в домене.



Установка сетевых компонентов

При настройке сетевых компонентов есть два варианта настройки: "Типичные параметры" и "Особые параметры". При выборе варианта "Типичные параметры" компьютер будет автоматически настроен на использование протокола TCP/IP с IP-адресом, получаемым от DHCP сервера автоматически. Если необходимо добавить другие протоколы или настроить протокол TCP/IP на использование постоянного адреса, выберите "Особые параметры".



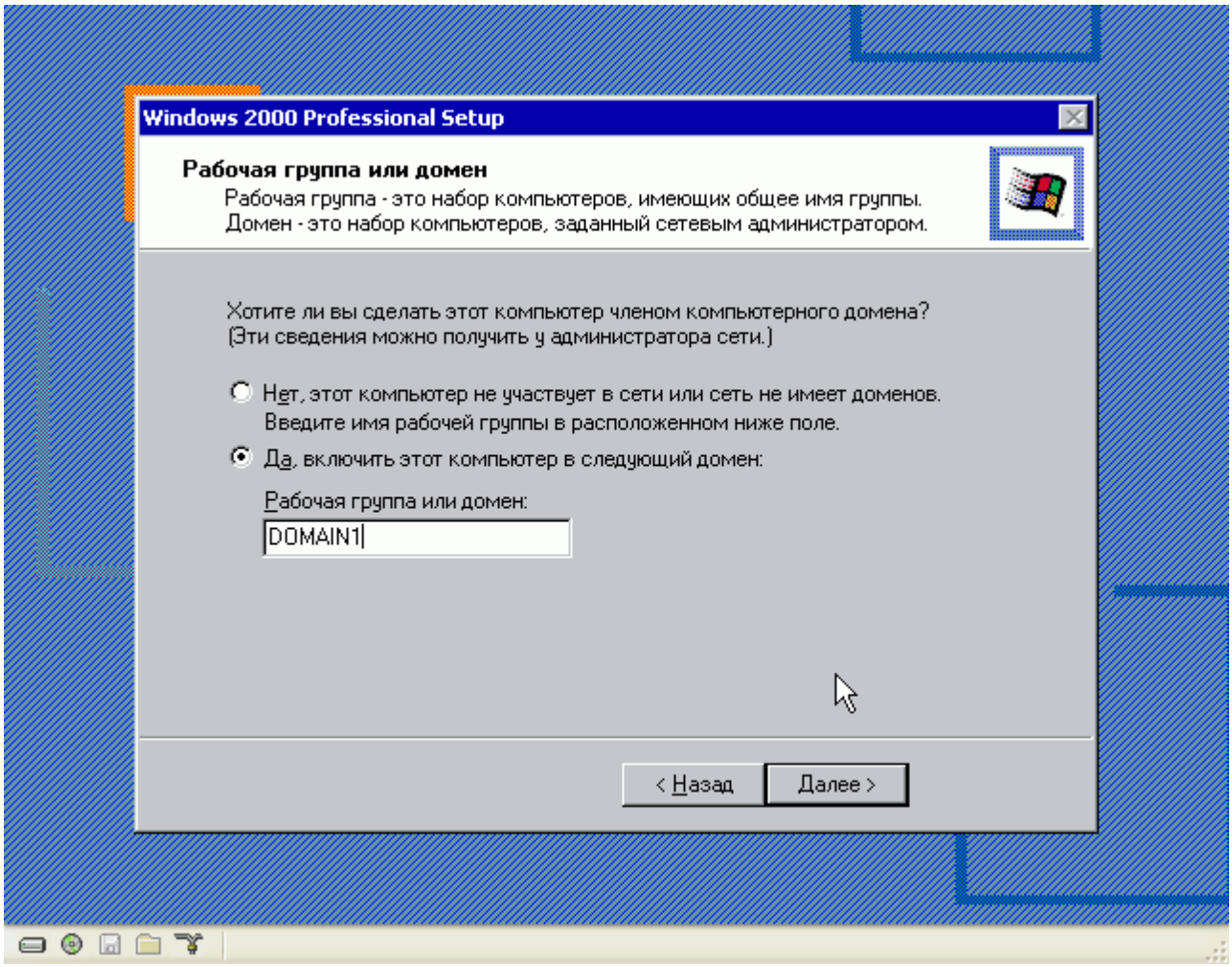
Присоединение к рабочей группе или домену

При установке системы Windows 2000 требуется присоединить компьютер к рабочей группе или домену.

Домен — это централизованно управляемая система, хранящая информацию о сетевых ресурсах и их потребителях (пользователях). ***Рабочая группа*** — это набор персональных компьютеров с общими папками и принтерами, в отличие от домена управляемая не администратором, а всеми владельцами компьютеров, входящих в рабочую группу. Для всех случаев, кроме небольших сетей с несколькими пользователями, рекомендуется использование доменов.

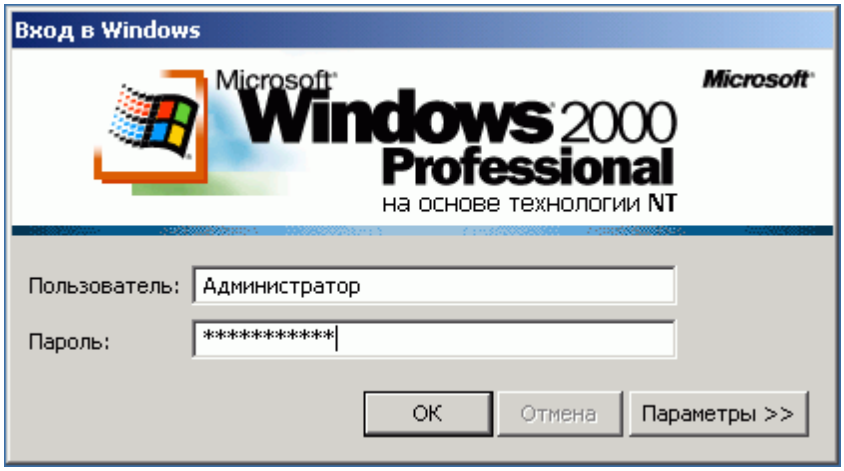
В рабочих группах может потребоваться, чтобы пользователи помнили пароли для каждого сетевого ресурса. В домене работа с паролями и разрешениями упрощается, так как в домене имеется единственная централизованная база данных с учетными записями пользователей, разрешениями и другими сетевыми данными. Между контроллерами домена автоматически производится репликация сведений, содержащихся в этой базе данных. Пользователь имеет возможность определить, какие серверы необходимо сделать контроллерами домена, а какие — его рядовыми членами. Эти роли могут быть определены как во время, так и после установки.

Если в сети существует домен Active Directory, необходимо подключить рабочую станцию к домену, но для этого необходимо знать имя учетной записи и пароль администратора домена. Если в настоящее время в сети еще нет ни одного контроллера домена Active Directory или сейчас нет возможности подключить к нему рабочую станцию, выбирайте подключение к рабочей группе. Подключение к домену можно выполнить и после установки Windows 2000.



Первый вход в систему

По завершению настроек и копирования файлов компьютер появится сообщение о том, что установка Windows 2000 завершена и компьютер необходимо перезагрузить. После перезагрузки войдите в систему с именем "Администратор" и паролем, который был указан во время установки.



Упражнение 1.A: "Установка Windows 2000 Professional"

Краткое описание

В этом упражнении Вы научитесь устанавливать на компьютер операционную систему Windows 2000 Professional.

Предварительные требования к выполнению упражнения

Для установки необходимо иметь компакт-диск Windows 2000 Professional и ключ продукта, который подходит к данной версии Windows 2000 Professional.

Порядок выполнения упражнения

1. Загрузите компьютер с компакт-диска Windows 2000 Professional, как описано в занятии 4.
2. На экране **Уведомление программы установки** нажмите **Enter**.
3. На экране **Вас приветствует программа установки** нажмите **Enter**. Если появится экран с сообщением о том, что жесткий диск новый или его содержимое стерто, нажмите **C**, чтобы продолжить работу.
4. На экране **Лицензионное соглашение Windows 2000** прочитайте текст соглашения и, если вы согласны с его условиями, нажмите **F8** для продолжения установки.
5. Когда на экране появится список имеющихся разделов, нажмите **C**, чтобы создать раздел на диске 0.
6. Когда Вам будет предложено выбрать размер раздела, в поле **Создать раздел размером (МБ)** удалите имеющееся значение, введите ***2048*** и нажмите **Enter**.
7. Находясь в списке имеющихся разделов, нажмите **Enter**, чтобы выбрать раздел **Новый (неформатированный) 2047 МБ**. Программа установки отобразит список параметров форматирования раздела.
8. Нажмите **Enter**, чтобы выбрать параметр **Форматировать раздел в системе NTFS**. Программа установки отформатирует раздел, проверит жесткий диск, и скопирует файлы на него для установки системы Windows 2000.
9. Оставьте в дисководе компакт-диск Windows 2000 Professional. Компьютер перезагрузится.
10. На экране **Вас приветствует мастер установки Windows 2000 Professional** нажмите **Далее**, или подождите несколько секунд, и процесс установки продолжится автоматически. Появится экран **Установка устройств**, на котором вам предлагается подождать, пока программа установки выявит и установит устройства.
11. На экране **Язык и стандарты** можно настроить Windows 2000 на использование различных языков. Нажмите нижнюю кнопку **Настроить** (Настройка переключения клавиатуры), выберите **Английский**(подсвечиваем параметр), нажмите **Язык по умолчанию**, затем **ОК**. Нажмите **Далее**.
12. На экране **Настройка принадлежности программ** в поля **Имя** и **Организация** введите соответственно Ваше имя и название организации, нажмите **Далее**.
13. На экране **Ключ продукта** введите ***номер продукта*** устанавливаемой версии Windows 2000 Professional.
14. На экране **Имя компьютера и пароль администратора** введите имя компьютера: ***Test01***,

пароль и подтверждение пароля: ***password***, после чего нажмите **Далее**.

15. На экране **Настройка времени и даты** установите дату, время и часовой пояс для Вашего компьютера, и затем нажмите **Далее**. Появится экран **Сетевые параметры**, на котором сообщается, что система Windows 2000 устанавливает сетевые компоненты, и затем предлагается выбрать вариант установки сети.
16. На экране **Сетевые параметры** установите переключатель **Типичные параметры** и нажмите **Далее**.

    Внимание! На экране **Сетевые параметры Далее** нужно нажать только один раз. Если нажать **Далее** дважды, Вы пропустите экран **Рабочая группа или домен**.
17. На экране **Рабочая группа или домен** предлагается присоединить компьютер к домену или рабочей группе. Убедитесь, что установлен переключатель **Нет, этот компьютер не участвует в сети, или сеть не имеет доменов**, и в поле **Рабочая группа или домен** стоит название рабочей группы: ***WORKGROUP***, и нажмите **Далее**. Появится экран **Установка компонентов**, на котором сообщается, что идет установка компонентов системы Windows 2000. Затем появится экран **Выполнение заключительных действий** с сообщением о том, что программа установки выполняет завершающие действия.
18. На экране **Завершение установки Windows 2000** нажмите **Готово**. Компьютер перезагрузится.

Тема 2

Основные инструменты администратора Windows 2000.

В этой теме:

Рассматриваются основы управления пользователями и группами, и предоставление им доступа к общим папкам и принтерам по сети. Разбираются вопросы администрирования сетевой печати. Рассматриваются способы и инструменты для наблюдения за работой серверов под управлением Windows 2000. Описываются способы архивирования и восстановления данных, процедуры обслуживания жестких дисков и возможности автоматизации задач.

Занятие 1: "Управление пользователями и группами"

Учетные записи пользователя позволяют индивидуальным пользователям получать доступ к сетевым ресурсам. Учетная запись пользователя - это однозначно определенный набор учетных данных, который распознается сетью. Администратор создает учетную запись пользователя для каждого, кто регулярно пользуется сетью. Администратор также назначает и поддерживает имена пользователя и пароли для каждой учетной записи пользователя. В операционной системе Windows 2000 существуют учетные записи пользователя двух видов: локальные учетные записи пользователя и учетные записи пользователя домена.

Локальная учетная запись пользователя создается в локальной базе учетных записей отдельно взятого компьютера, что дает пользователю возможность входить на конкретный компьютер и получать доступ к ресурсам этого компьютера. Если компьютер не является контроллером домена, учетная запись хранится только на этом локальном компьютере. С помощью этой учетной записи пользователь получает доступ только к ресурсам данного компьютера.

С помощью учетной записи пользователя домена пользователь может входить в домен для доступа к сетевым ресурсам. Пользователь, имеющий учетную запись домена, может получить доступ ко всем ресурсам этого домена.

Группа - это набор учетных записей пользователя. Разрешения на доступ можно задать одновременно всем членам группы, и нет необходимости задавать их индивидуально. Обеспечив доступ для группы, потом можно просто добавлять в эту группу соответствующих пользователей. Можно использовать принятые по умолчанию или встроенные группы, предлагаемые операционной системой Windows 2000, либо создать новые группы в соответствии с потребностями организации.

Группа может существовать на локальном компьютере, или на компьютерах в пределах одного домена , или на компьютерах в пределах нескольких доменов.

Локальные учетные записи

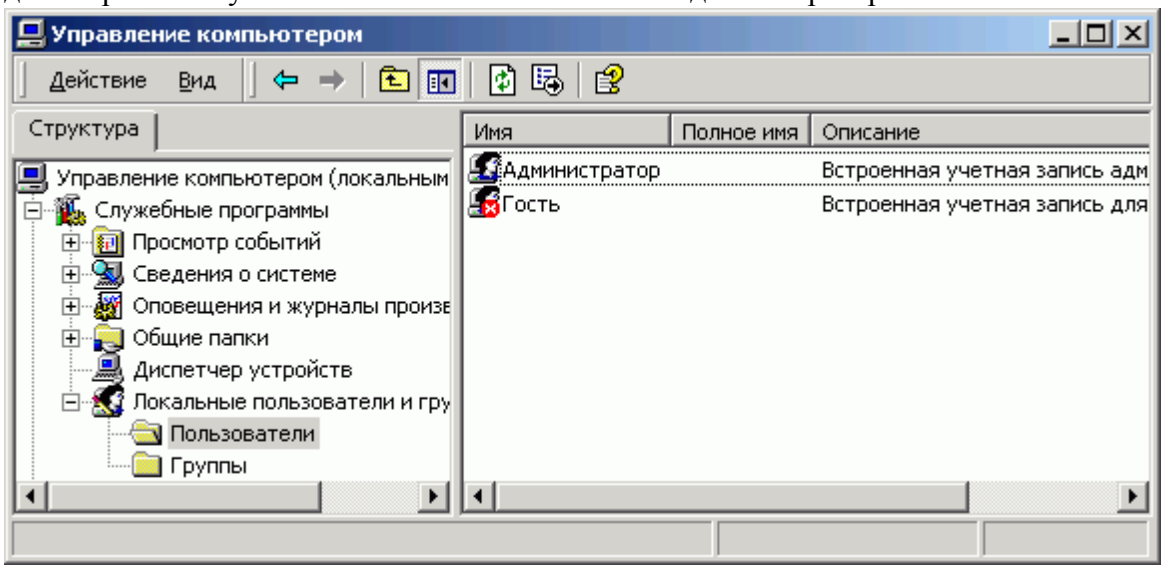
Чтобы получить доступ к ресурсам локального компьютера, пользователю нужно иметь локальную учетную запись на этом компьютере. Локальные учетные записи пользователя бывают двух видов: учетные записи, определяемые пользователем, и встроенные учетные записи. При создании учетной записи она существует только в локальной базе данных безопасности соответствующего компьютера.

Учетная запись, определяемая пользователем

Учетные записи, определяемые пользователем - это те учетные записи, которые администратор создает, чтобы дать пользователю доступ только к тем компьютерам, где у этого пользователя есть учетная запись. Локальные учетные записи пользователя можно создавать на рядовых серверах и на компьютерах, работающих под управлением операционной системы Windows 2000 Professional, но не являющихся контроллерами домена. Локальная учетная запись пользователя применяется только на автономных компьютерах или на компьютерах в небольших сетях, например, в рабочей группе. Пользователь может иметь одну учетную запись на локальном компьютере, а другую - в домене, но он не может работать с ними двумя одновременно. В момент входа на компьютер пользователь указывает, с какой записью он будет работать.

Встроенные (локальные) учетные записи пользователя

Помимо учетных записей, определяемых пользователем, операционная система Windows 2000 предоставляет две встроенных учетных записи пользователя, чтобы помочь администраторам в выполнении задач администрирования и для предоставления пользователям возможности временного доступа на локальный компьютер. Операционная система Windows 2000 в процессе установки создает две встроенных учетных записи пользователя - "Администратор" и "Гость".



"Администратор"

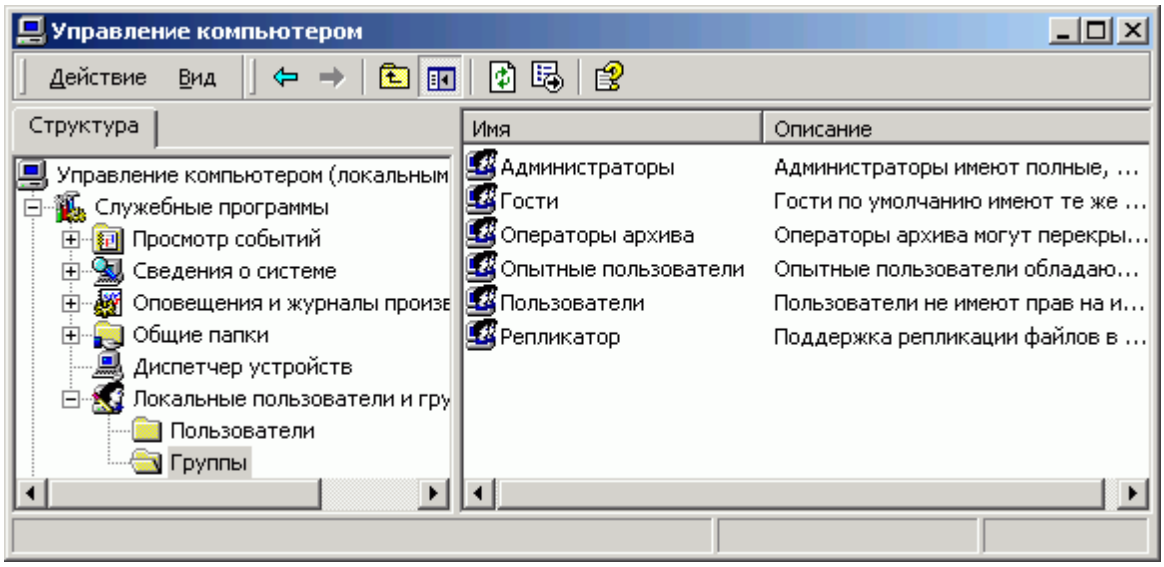
Администратор с помощью учетной записи "Администратор" создает для себя учетную запись пользователя на компьютере, где впервые установлена операционная система Windows 2000. Встроенная учетная запись "Администратор" не может быть ни удалена, ни отключена. Это гарантирует, что администратору не будет блокирован доступ к компьютеру. Учетная запись "Администратор" требует пароля, который администратор задает в процессе установки.

"Гость"

Пользователи, не имеющие своей учетной записи на компьютере, могут войти на него с использованием учетной записи "Гость". Этой же учетной записью могут воспользоваться и те, чья учетная запись отключена. Чтобы пользователь мог войти как "Гость", администратор должен включить эту учетную запись, поскольку она по умолчанию отключена. Эта учетная запись пароля не требует.

Группы на локальном компьютере

На компьютерах, не являющихся контроллерами домена, можно создавать только локальные группы в локальной базе данных безопасности. Группа, расположенная на компьютере, не являющемся контроллером домена, обеспечивает безопасность и доступ только для этого локального компьютера. Например, чтобы дать пользователю права администратора на локальном компьютере, достаточно его добавить в группу "Администраторы" данного компьютера с помощью инструмента "Локальные пользователи и группы" .



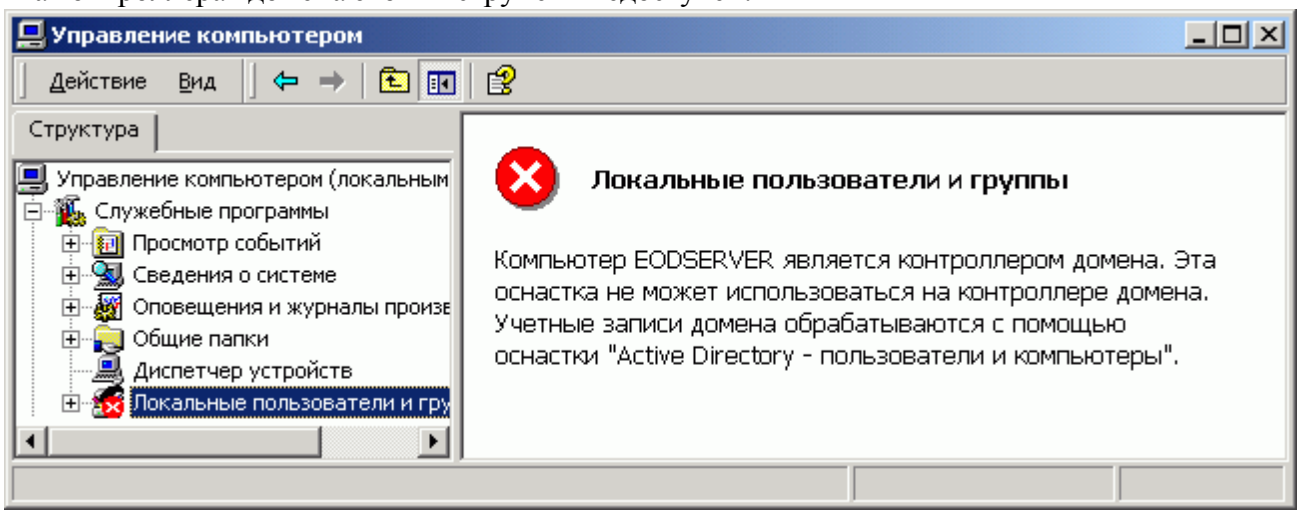
Инструмент "Локальные пользователи и группы"

Операционная система Windows 2000 предоставляет в распоряжение администратора инструмент "Локальные пользователи и группы", который позволяет управлять учетными записями пользователей на локальном компьютере. Инструмент "Локальные пользователи и группы" доступен на компьютерах, работающих под управлением системы Windows 2000 Professional и на рядовых серверах, работающих под управлением системы Windows 2000 Server. С помощью инструмента "Локальные пользователи и группы" можно выполнять следующие операции:

- создавать новую учетную запись пользователя или удалять существующую;
- изменять учетную запись пользователя, меняя имя пользователя или другие данные учетной записи, такие как пароль или описание;
- сбрасывать пароль для учетной записи пользователя;
- отключать или включать учетную запись.

Чтобы использовать инструмент "Локальные пользователи и группы", в **панели управления** локального компьютера, не являющегося контроллером домена, последовательно выберите **Администрирование**, **Управление компьютером** и **Локальные пользователи и группы**.

На контроллерах домена этот инструмент недоступен.



Для закрепления навыков по управлению локальными учетными записями пользователей и групп выполните упражнение А.

Учетные записи пользователя домена

Локальная учетная запись пользователя дает пользователю возможность входить на локальный компьютер для доступа к локальным ресурсам. Однако в сетевой среде пользователям нужен доступ к сетевым ресурсам. Для доступа к ним необходима учетная запись пользователя домена. Когда создается учетная запись пользователя домена, она помещается в службу каталогов Active Directory и доступна с любого компьютера, принадлежащего к этому домену. В рабочей группе, наоборот, учетная запись пользователя существует только на локальном компьютере.

Учетные записи пользователя домена, определяемые пользователем

Учетные записи пользователя домена, определяемые пользователем - это учетные записи, которые администратор создает для того, чтобы пользователи могли входить в домен и получать доступ к ресурсам сети. Учетные записи пользователя домена, определяемые пользователем, создаются на контроллере домена. Этот контроллер домена реплицирует данные новой учетной записи пользователя на все контроллеры в домене. При входе пользователь указывает имя учетной записи пользователя и пароль, а также домен, в котором существует эта учетная запись. Первый доступный контроллер домена использует введенные данные для проверки подлинности учетной записи пользователя.

Встроенные учетные записи пользователя домена

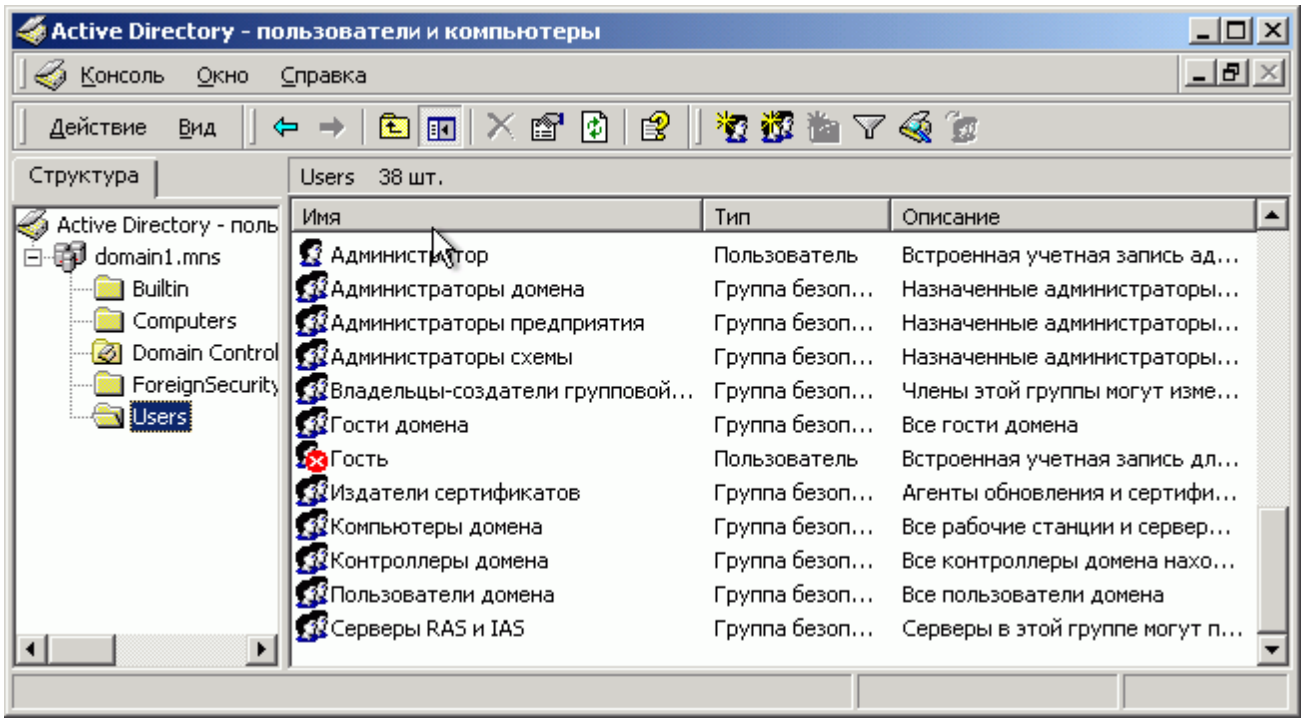
Операционная система Windows 2000 предлагает две встроенные учетные записи пользователя домена - "Администратор" и "Гость". Они подобны встроенным учетным записям пользователя, существующим на локальных компьютерах в рабочих группах. Главное отличие состоит в том, что эти учетные записи дают возможность доступа в домен.

"Администратор"

Встроенная учетная запись "Администратор" управляет всей конфигурацией компьютера и домена. Пользуясь этой записью, администратор может создавать учетные записи пользователя и группы, управлять безопасностью, распоряжаться принтерами и назначать разрешения учетным записям пользователей. Эту учетную запись можно переименовать, но нельзя удалить.

"Гость"

Встроенная учетная запись "Гость" позволяет временным пользователям получить доступ к сетевым ресурсам. Например, в системе с низким уровнем безопасности сотрудник, которому нужен кратковременный доступ к ресурсам, может воспользоваться учетной записью "Гость". По умолчанию эта учетная запись является отключенной.



Группы на контроллере домена

На контроллере домена группы создаются в службе каталогов Active Directory. Группа, расположенная на контроллере домена, может включать в себя пользователей одного или нескольких доменов. Например, чтобы предоставить пользователям права администратора на контроллер домена, их добавляют в локальную группу "Администраторы" на контроллере домена с помощью инструмента "Active Directory - пользователи и компьютеры".

Инструмент "Active Directory - пользователи и компьютеры"

Для управления учетными записями пользователей в службе каталогов Active Directory существует инструмент под названием "Active Directory - пользователи и компьютеры".

Этот инструмент установлен на компьютерах, настроенных как контроллеры домена. Для работы с инструментом "Active Directory - пользователи и компьютеры" необходимо войти в домен Windows 2000 (не на локальный компьютер), имея при этом достаточные права для выполнения операций по управлению учетными записями.

С помощью инструмента "Active Directory - пользователи и компьютеры" можно выполнять в домене следующие операции:

- добавлять или удалять учетные записи пользователя;
- включать и отключать учетные записи пользователя;
- находить или перемещать учетные записи пользователя;
- переименовывать учетные записи пользователя;
- сбрасывать пароли пользователей.

Чтобы использовать инструмент "Active Directory - пользователи и компьютеры", в **панели управления** последовательно выберите **Администрирование**, **Active Directory - пользователи и компьютеры**.

Более подробно применение этого инструмента разбирается в теме 6 "Администрирование Active Directory".

Упражнение 2.А: "Создание локальных пользователей и групп"

Краткое описание

В этом упражнении Вы научитесь создавать учетные записи пользователей и групп на Windows 2000 Professional.

Предварительные требования к выполнению упражнения

Необходимо иметь компьютер с установленной операционной системой Windows 2000 Professional (то есть выполнить упражнение 1.А), на которую Вы имеете права локального администратора.

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.А по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. В **Панели управления** локального компьютера последовательно выберите: **Администрирование**, **Управление компьютером** и **Локальные пользователи и группы**.
3. Правой кнопкой щелкните на папке **Пользователи** и выберите **Новый пользователь...**
4. В поле **Пользователь** введите ***vpupkin***, а в поле **Полное имя** введите ***Пупкин Василий Иванович***.
5. Снимите флажок **Потребовать смену пароля при следующем входе в систему** и введите в поле **Пароль** и **Подтверждение пароля** ***userpassword***
6. Нажмите **Создать** и повторите процедуру добавления пользователя, введя в поле **Пользователь** ***admin***, в поле **Полное имя** введите ***Админов Александр Федорович***. Пароль для этого пользователя - ***adminpassword***.
7. Нажмите **Закрыть** и правой кнопкой щелкните на папке **Группы** и выберите **Новая группа...**
8. В поле **Имя группы** введите ***Кадры***. Нажмите **Добавить...** и добавьте в члены этой группы пользователя ***vpupkin***.
9. Нажмите **Создать**, а затем **Закрыть**.
10. Откройте папку **Группы** и дважды щелкните на группе **Администраторы**. Нажмите **Добавить...** и добавьте в члены этой группы пользователя ***admin***.

Занятие 2: "Управление печатью"

Windows 2000 позволяет работать с ресурсами печати пользователям всей сети. Клиенты, использующие различные компьютеры и операционные системы, могут отправлять задания на печать на принтеры, подключенные локально к серверу печати Windows 2000, расположенные в Интернете, или подключенные к сети посредством встроенных или внешних сетевых плат или через другой сервер.

Windows 2000 поддерживает некоторые дополнительные возможности печати. Например, сервер печати Windows 2000 допускает удаленное администрирование. Другой удобной возможностью является отсутствие необходимости в ручной установке драйвера принтера на клиентский компьютер Windows 2000, на котором нужно использовать принтер. Драйвер загружается автоматически при подключении клиента к серверу печати Windows 2000.

Терминология

Чтобы понимать, как настраивается печать в Windows 2000, необходимо знать следующие термины:

Устройство печати - это аппаратное устройство, осуществляющее печать документов (то, что обычно называется принтером). Оно может быть подключено к физическому порту компьютера (обычно LPT1) или к сети с использованием специализированного сетевого адаптера (например, JetDirect).

Принтер - это программный интерфейс между операционной системой и устройством печати. Принтер определяет, какое устройство печати должно использоваться: на локальном порту, на порту для сетевого подключения или печать производится в файл.

Сервер печати - компьютер, на котором располагаются принтеры и драйверы клиента. Сервер печати принимает и обрабатывает документы, поступающие с клиентских компьютеров. Администратор устанавливает на сервере печати сетевые принтеры, связанные с локальными и сетевыми устройствами печати, и организует общий доступ к ним.

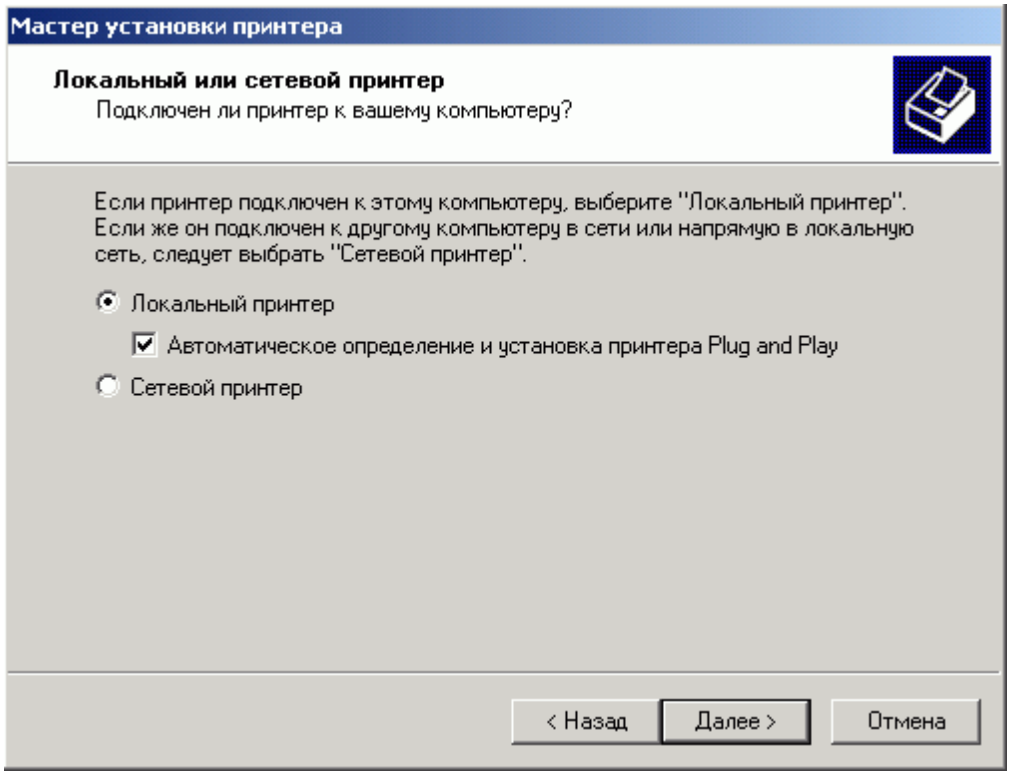
Драйвер принтера - набор файлов, содержащий данные, необходимые системе Windows 2000 для преобразования команд печати в язык конкретного принтера. Такое преобразование дает устройству печати возможность распечатать документ. Драйвер принтера специфичен для каждой модели устройства печати, и на сервере печати должен находиться соответствующий драйвер принтера.

Установка принтера и предоставление общего доступа к нему для локального устройства печати

Последовательно выберите **Пуск**, **Настройка** и **Принтеры**. Дважды щелкните значок **Установка принтера**, чтобы запустить мастер установки принтера, и нажмите **Далее**.

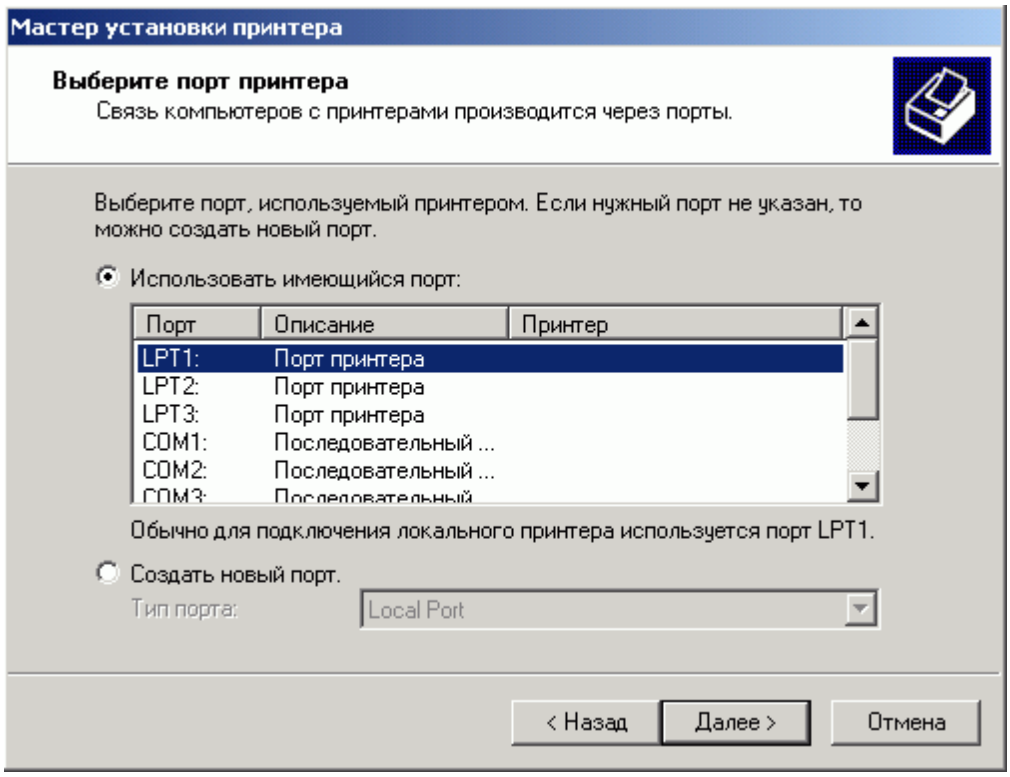
Локальный или сетевой принтер

Выберите **Локальный принтер**. Этот параметр означает, что принтер добавляется к компьютеру, за которым вы находитесь (к серверу печати).



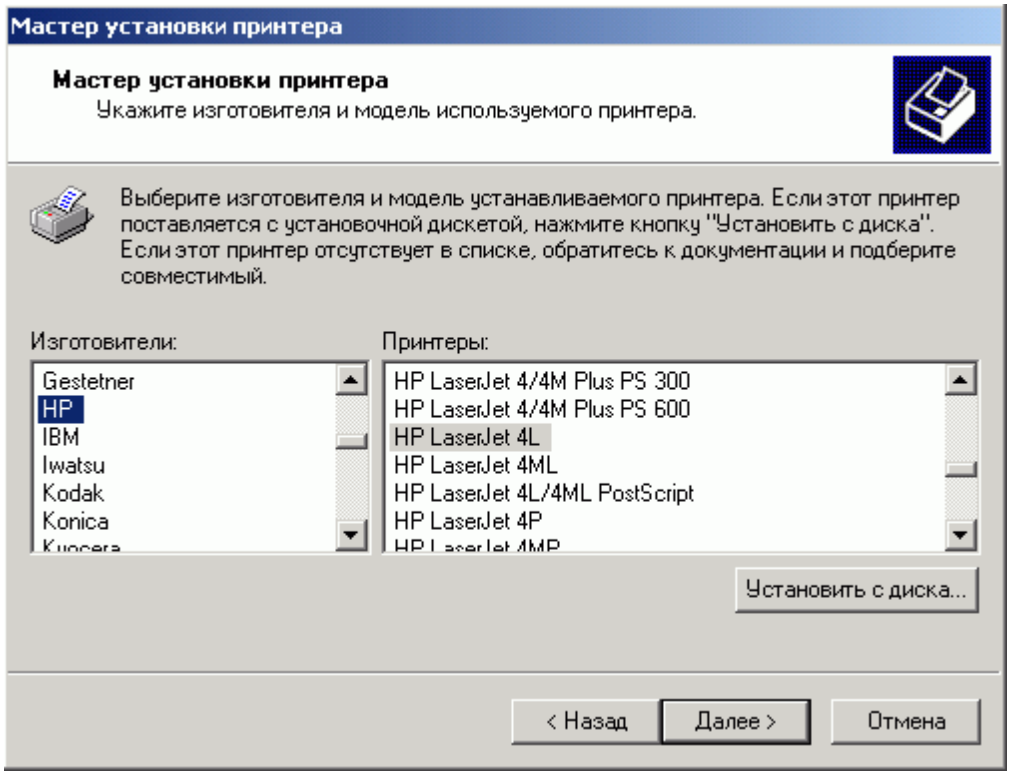
Выберите порт принтера

Установите флажок слева от пункта **Использовать имеющийся порт** и укажите порт сервера печати, к которому присоединено устройство печати (локальные устройства печати обычно используют LPT1). Можно также добавить дополнительный порт, что позволит вести печать через нестандартные порты оборудования, например, по протоколу LPR (протокол печати для UNIX).



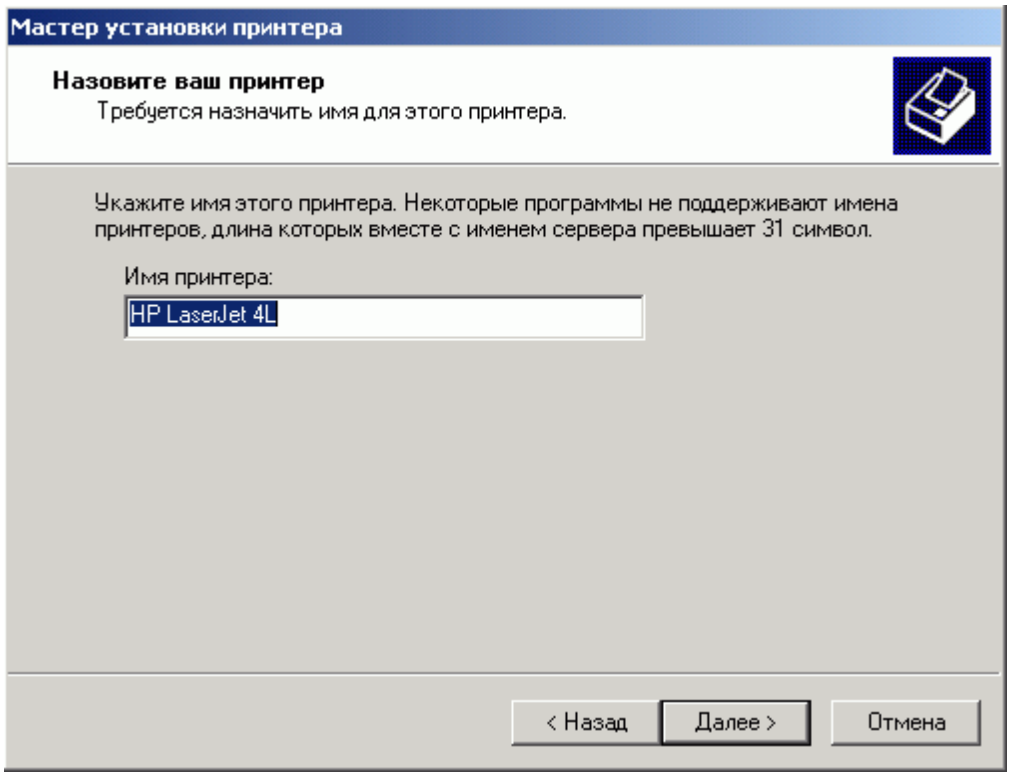
Изготовитель и модель принтера

Укажите правильный драйвер принтера для локального устройства печати. Если имеющееся устройство печати не входит в предлагаемый список, необходимо установить драйвер принтера, поставляемый изготовителем или выбрать модель, для которой используется тот же драйвер.



Имя принтера

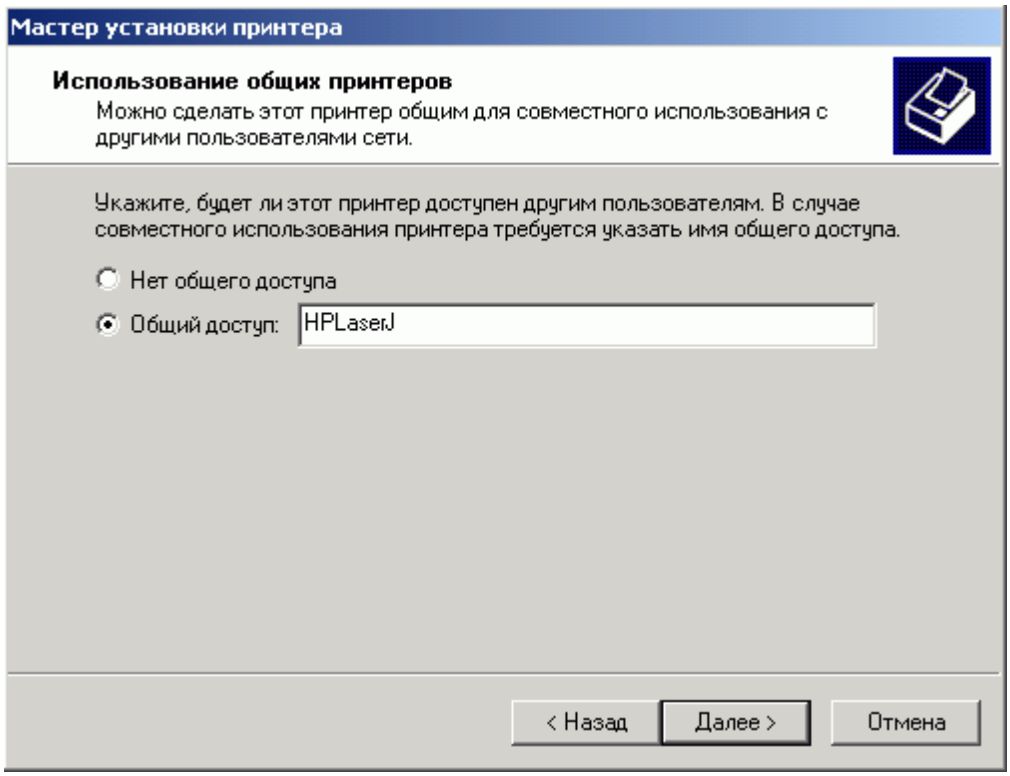
Здесь необходимо установить имя, определяющее принтер для пользователей. Следует использовать интуитивно понятное имя, описывающее устройство печати. Это имя также выдается в результате поиска по службе каталогов Active Directory.



Общий доступ к принтеру

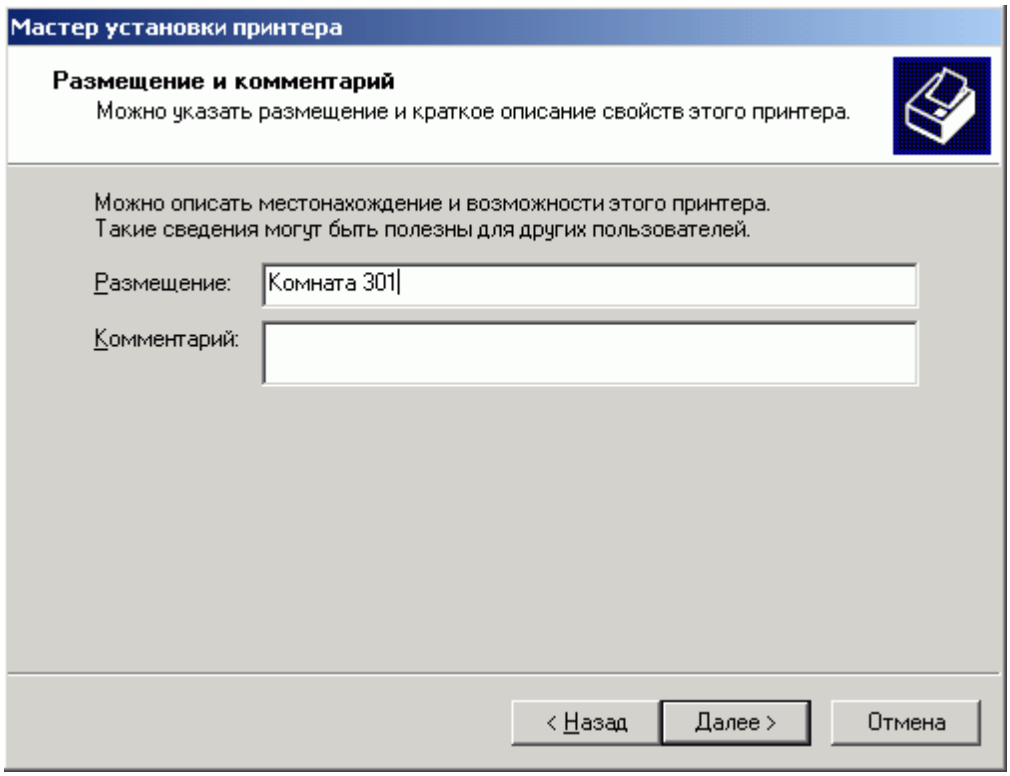
Здесь нужно указать имя общего ресурса, по которому пользователи (имеющие соответствующее разрешение на доступ) смогут подключиться к принтеру по сети. Это имя отображается, когда пользователь ищет принтер или указывает путь к принтеру.

Проверьте, что имя общего ресурса для принтера совместимо с соглашениями об именах для всех клиентских компьютеров в сети. По умолчанию имя общего ресурса сокращается до вида 8.3 знаков. Если использовать имя общего ресурса, превышающее 8.3 знаков, некоторые клиентские компьютеры не смогут подключиться к этому принтеру.



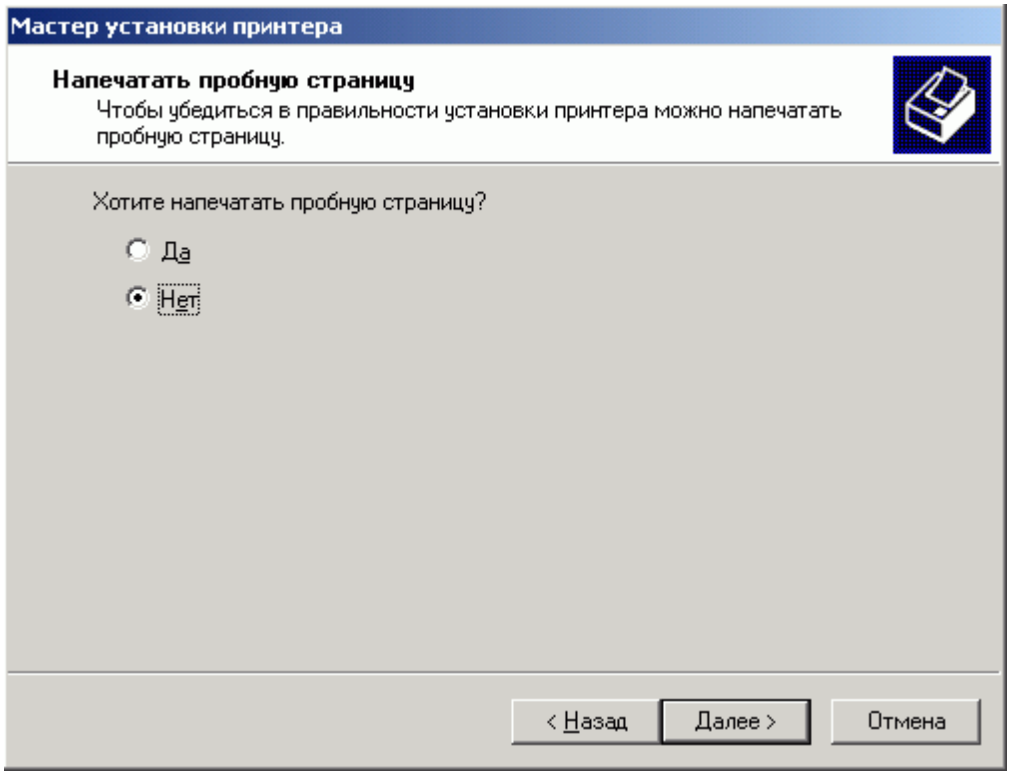
Размещение и Комментарий

Здесь нужно ввести информацию, которая позволит пользователям определить, соответствует ли устройство печати их потребностям. По введенной в этих параметрах информации пользователи могут вести поиск в службе каталогов Active Directory. Необходимо задавать эту информацию в стандартном виде, чтобы пользователи могли сделать обоснованный выбор по результатам поиска.



Пробная страница

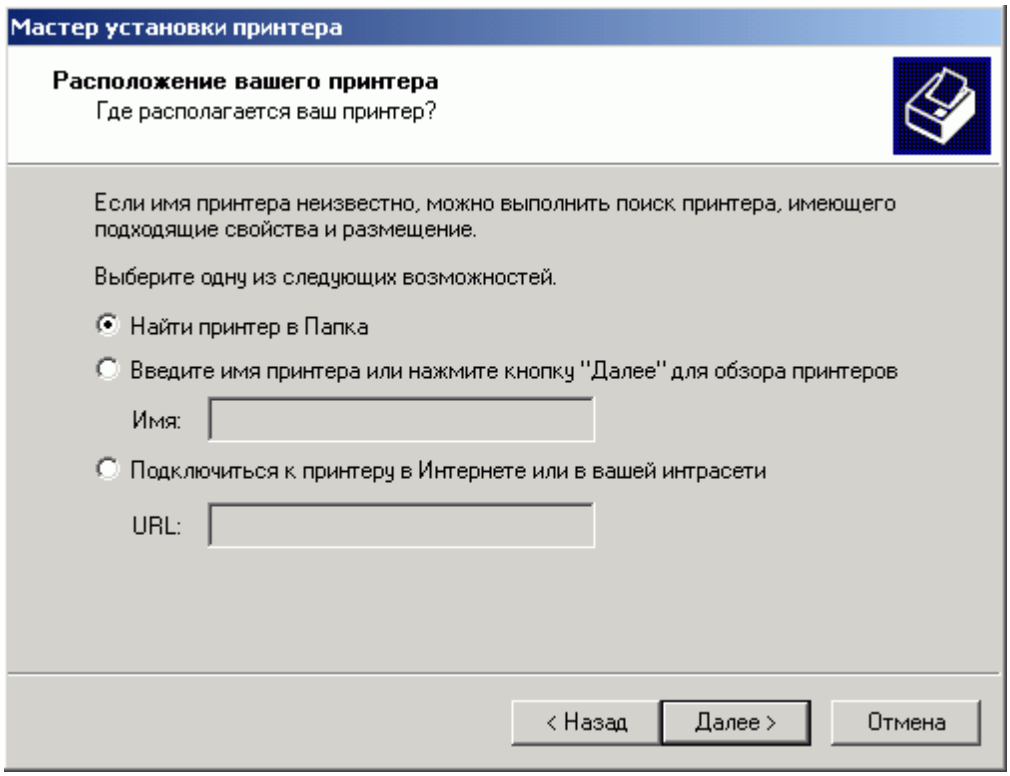
Предназначается для проверки правильности установки принтера. Чтобы распечатать пробную страницу, установите переключатель на **Да**.



Установка принтера и предоставление общего доступа к нему для устройства печати с сетевым интерфейсом

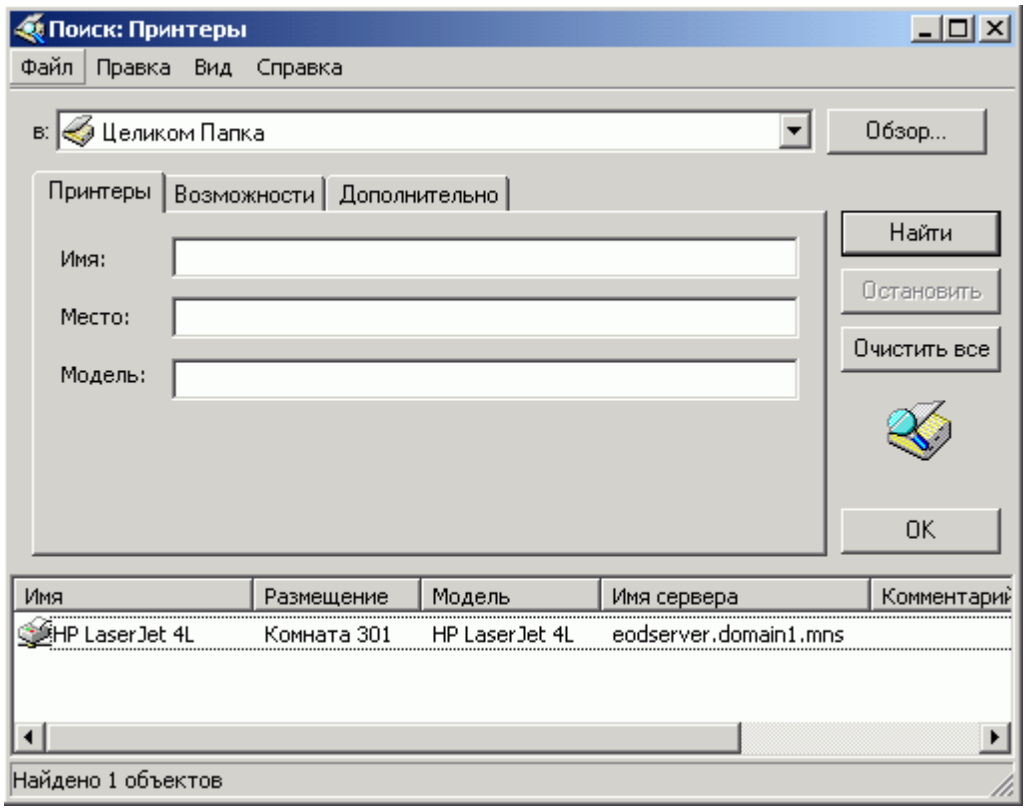
Процесс установки сетевого принтера почти не отличается от установки локального принтера. Если подключаемый принтер доступен только по протоколу TCP/IP, нужно выбрать пункт **Локальный принтер** и создать новый TCP/IP порт. Если же необходимо подключиться к принтеру, который предоставлен в общий доступ на сервере Windows 2000 - выбираем пункт **Сетевой принтер** и вместо выбора порта необходимо указать, какой из принтеров, доступных по сети или через Интернет, должен быть установлен.

При добавлении сетевого принтера и предоставлении общего доступа к нему система Windows 2000 автоматически публикует принтер в службе каталогов Active Directory. После этого пользователи могут искать этот принтер в службе каталогов Active Directory.



Поиск принтера

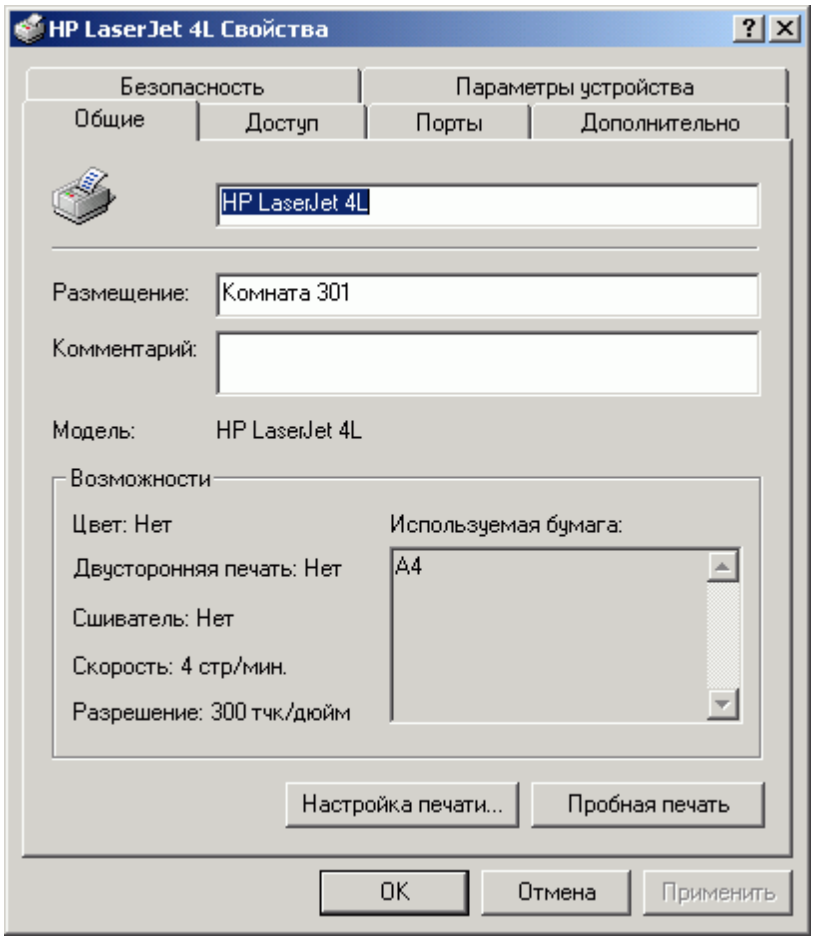
1. Чтобы открыть окно поиска принтеров, нажмите **Пуск** и последовательно выберите команды **Найти**, **Принтеры**.
2. В поле **в** выберите домен, в котором требуется выполнить поиск, или нажмите **Обзор**, чтобы выбрать нужный домен. Если выбрать **Полностью Active Directory**, то сузить область поиска с помощью вкладки **Дополнительно** будет нельзя.
3. Введите условия поиска на вкладках **Принтеры**, **Возможности** и **Дополнительно**.
   - На вкладке **Принтеры** введите имя и модель принтера.
   - На вкладке **Возможности** можно указать дополнительные условия поиска, такие как возможность двусторонней печати или печати с определенным разрешением.
   - На вкладке **Дополнительно** задаются пользовательские или дополнительные поля, определяющие такие условия, как возможность разбора по копиям или поддержка определенного языка принтера.
4. Нажмите **Найти**, чтобы запустить поиск, или **Очистить все**, чтобы очистить поля условий поиска и начать новый поиск.



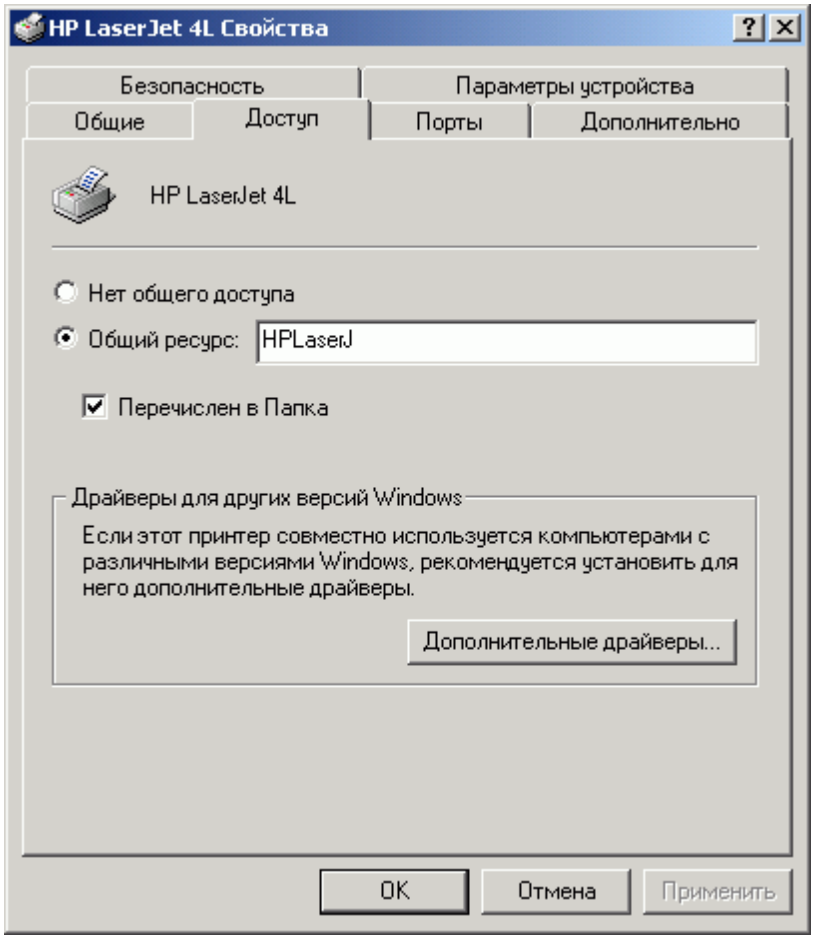
Настройка принтера

Для изменения настроек принтера после его установки щелкните правой кнопкой на объекте принтера и выберите **Свойства**.

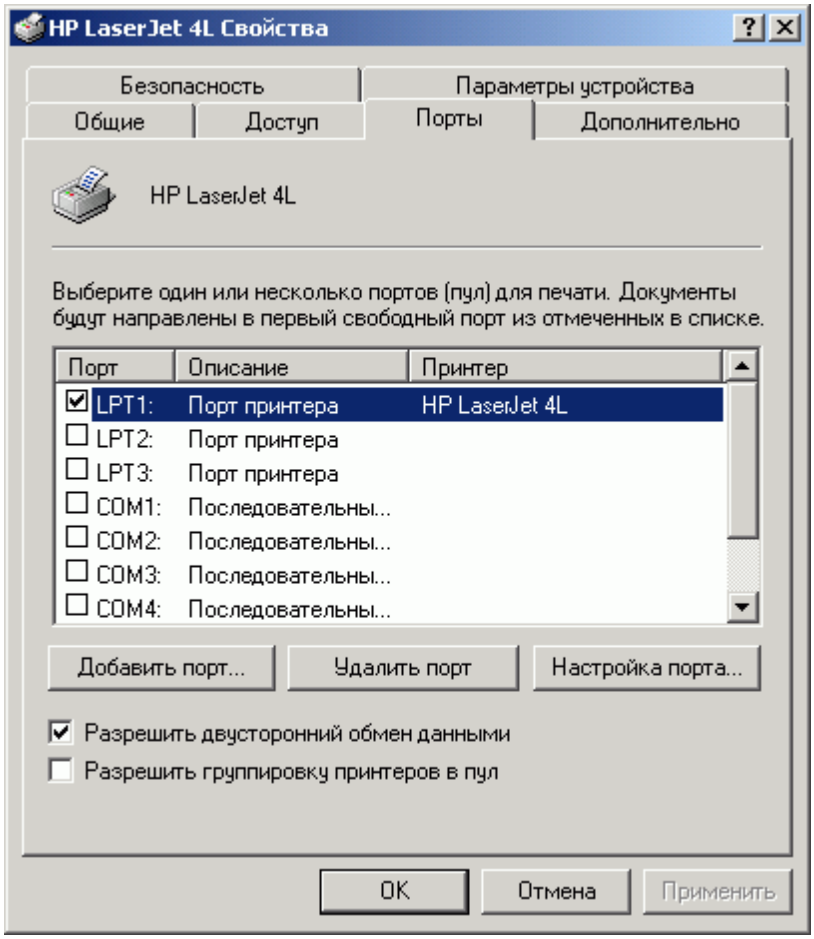
Закладка **Общие** позволяет измененить имя принтера, ввести новое расположение принтера, напечатать пробную страницу



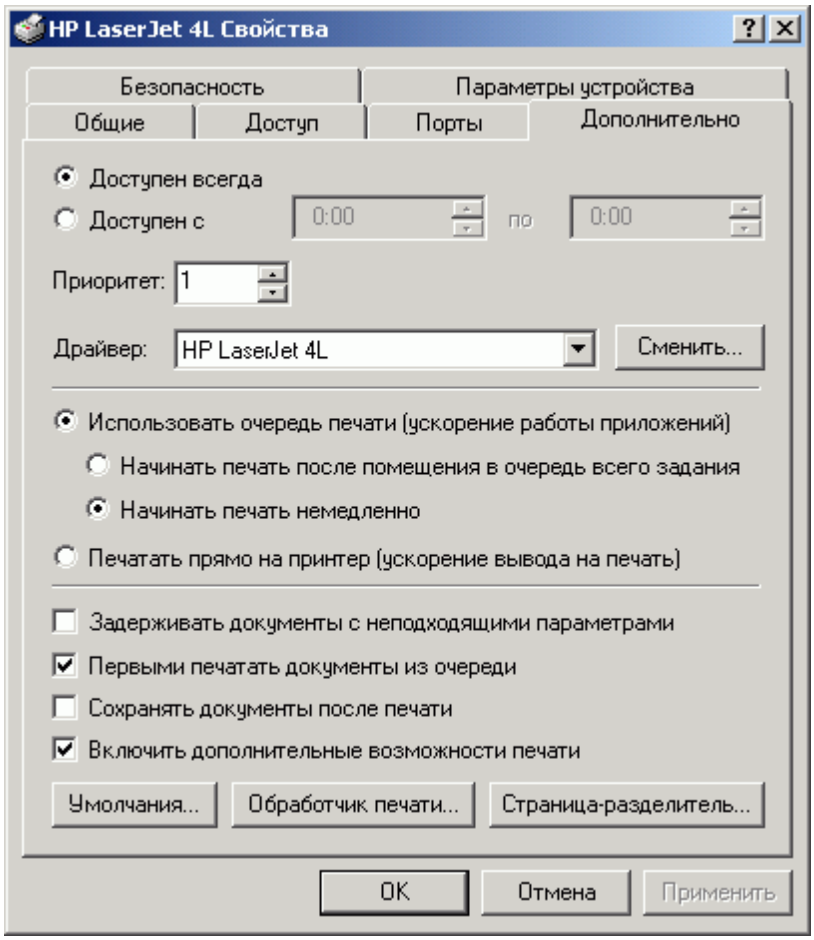
На закладке **Доступ** можно предоставить или отменить общий доступ к принтеру, контролировать публикацию сведений о принтере в Active Directory (флажок **Перечислен в Папка**), а также установливать дополнительные драйвера для клиентов печати с операционными системами, отличными от Windows 2000.



Закладка **Порты** предоставляет возможности по добавлению, удалению и настройке портов, через которые идет печать на принтер (в том числе и сетевые порты)



Больше всего настроек представлено на закладке **Дополнительно**: управление временем доступности принтера, назначение приоритетов принтера, изменение драйвера принтера, настройка параметров очереди печати, задание свойств печати по умолчанию.

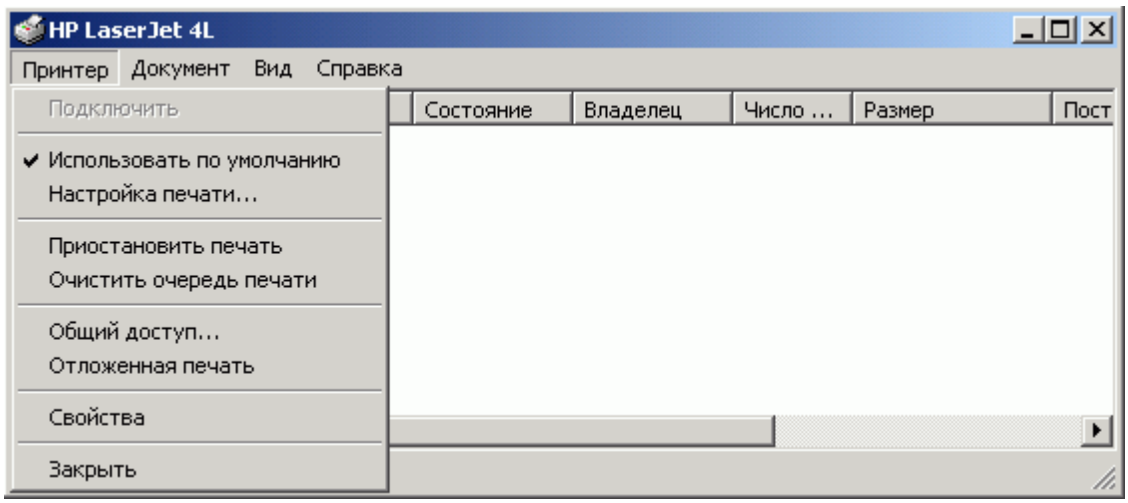


Управление принтерами и документами

Операции по управлению принтерами воздействуют на весь принтер, а не на отдельные документы. К ним относятся приостановка, возобновление и очистка очереди печати данного принтера. Чтобы управлять принтером, необходимо в папке **Принтеры** дважды щелкнуть используемый принтер, откроется очередь печати.

- Для приостановки выберите команду **Приостановить печать**. Когда принтер приостановлен, рядом с командой **Приостановить печать** появляется флажок. Чтобы возобновить печать и убрать флажок, снова выберите команду **Приостановить печать**.
- Чтобы отменить печать всех документов, щелкните на принтер, для которого нужно отменить печать всех документов, и выберите команду **Очистить очередь печати**.

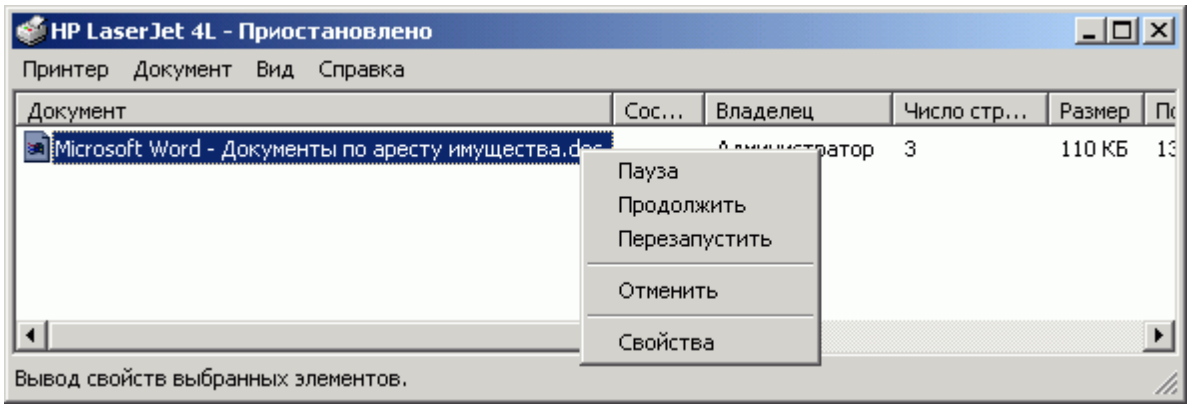
Для приостановки, возобновления или отмены печати на принтере необходимо иметь разрешение "Управление принтерами". Более подробно о правах доступа к принтеру см. [занятие 3](#).



Управление документом включает в себя: приостановку и возобновление печати, перезапуск печати документа с начала, удаление документа, а также просмотр и изменение различных параметров документа, например его приоритета или лица, которому отправляется уведомление о завершении печати этого документа. Чтобы управлять документами, в папке **Принтеры** дважды щелкните на используемый принтер, откроется очередь печати. На выбранном документе щелкните правой кнопкой мыши.

- Чтобы отменить печать документа, выберите команду **Отменить**
- Чтобы приостановить печать, выберите команду **Пауза**. Документ не будет печататься, пока печать не будет возобновлена.
- Чтобы возобновить печать, выберите команду **Продолжить**. Документ начнет печататься. Однако при наличии документов с более высокими приоритетами они будут напечатаны в первую очередь.
- Чтобы перезапустить печать документа, выберите команду **Перезапустить**.
- Чтобы изменить порядок печати документов, находящихся в очереди, выберите команду **Свойства**. На вкладке **Общие** перетащите ползунок **Приоритет**, чтобы установить необходимый приоритет документа. На этой же закладке можно просмотреть другие параметры документа.

Изменять порядок документов, ожидающих печати, можно только при наличии разрешения "Управление документами". Более подробно о правах доступа к принтеру см.[занятие 3](#).



Занятие 3: "Настройка доступа к ресурсам"

Предоставляя доступ к файловым ресурсам на компьютере, работающем под управлением Windows 2000, можно контролировать, кто будет иметь доступ к ресурсам и какого рода будет этот доступ. Для этого используются соответствующие разрешения. **Разрешения** определяют вид доступа к ресурсу, предоставленного пользователю или группе. Например, у пользователей из отдела кадров организации может возникнуть необходимость изменить документ, определяющий политику компании в области подбора персонала. Для этого администратор должен назначить соответствующие разрешения сотрудникам отдела кадров.

Для назначения разрешений на доступ к отдельным файлам и папкам в операционной системе Windows 2000 используется файловая система NTFS. Можно также управлять разрешениями, назначенными пользователям для доступа к общим папкам и сетевым принтерам.

Разрешения на доступ в файловой системе NTFS

Разрешения на доступ к файлам

Разрешения на доступ к файлам NTFS управляют доступом к отдельным файлам, указывая учетные записи пользователей, которые имеют право доступа к этим файлам, а также какого рода доступ они могут иметь.

В таблице перечислены стандартные разрешения на доступ к файлам NTFS и вид доступа, который дает каждое из них - от предельно ограниченного до наиболее свободного.

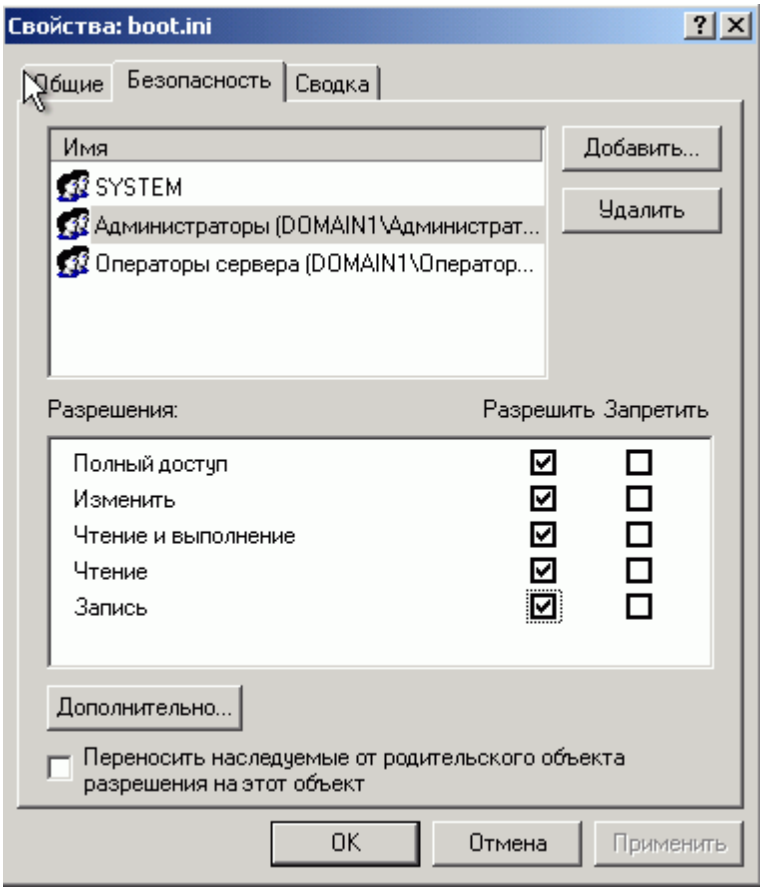
Разрешение на доступ к файлам NTFS	**Позволяет пользователю**
Чтение	Читать файл и просматривать его атрибуты, имя владельца и разрешения
Чтение и выполнение	Запускать приложения и выполнять действия, предусмотренные в разрешении на чтение
Запись	Перезаписывать содержимое файла, изменять его атрибуты и просматривать имя его владельца и разрешения
Изменение	Изменять и удалять файл, а также выполнять действия, предусмотренные в разрешении на запись и в разрешении на чтение и выполнение
Полный доступ	Изменять разрешения, владельца и выполнять действия, предусмотренные во всех остальных разрешениях на доступ к файлам NTFS

Проверка разрешений на доступ к файлам

Администратор назначает файлу разрешения из вкладки **Безопасность** диалогового окна **Свойства** файла. С помощью той же вкладки можно просмотреть текущие разрешения на доступ к файлу.

Чтобы перейти на вкладку **Безопасность**, выполните следующие действия.

1. В проводнике Windows щелкните файл правой кнопкой мыши, выберите **Свойства**.
2. В диалоговом окне **Свойства** перейдите на вкладку **Безопасность**.



Вкладка **Безопасность** состоит из двух разделов - **Имя** и **Разрешения**. В разделе **Имя** показан список пользователей и групп, имеющих разрешения на доступ к этому файлу. В разделе **Разрешения** показан список разрешений, которые можно дать или в предоставлении которых можно отказать пользователю или группе.

Обычно выбираются разрешения, которые требуется предоставить. Однако в некоторых случаях может оказаться проще указать разрешения, которые необходимо отменить. Например, предоставляя всем пользователям разрешение на доступ к файлам, может потребоваться ограничить доступ к этому ресурсу пользователей с учетной записью "Гость". Для этого следует отменить соответствующие разрешения для учетной записи "Гость".

Разрешения на доступ к папкам

Разрешения на доступ к папкам NTFS управляют доступом пользователя к папкам и содержащимся в них файлам и вложенным папкам. Если дано разрешение на доступ к папке, но не дано разрешение на доступ к файлу, находящемуся в папке, то запрет имеет преимущество над разрешением, относящимся к папке.

В таблице перечислены стандартные разрешения на доступ к папке NTFS и вид доступа, который предоставляет каждое из них - от самого ограниченного до наиболее свободного.

Разрешение на доступ к папке NTFS	**Позволяет пользователю**
Список содержимого папки	Просматривать имена файлов в папке и вложенных папок

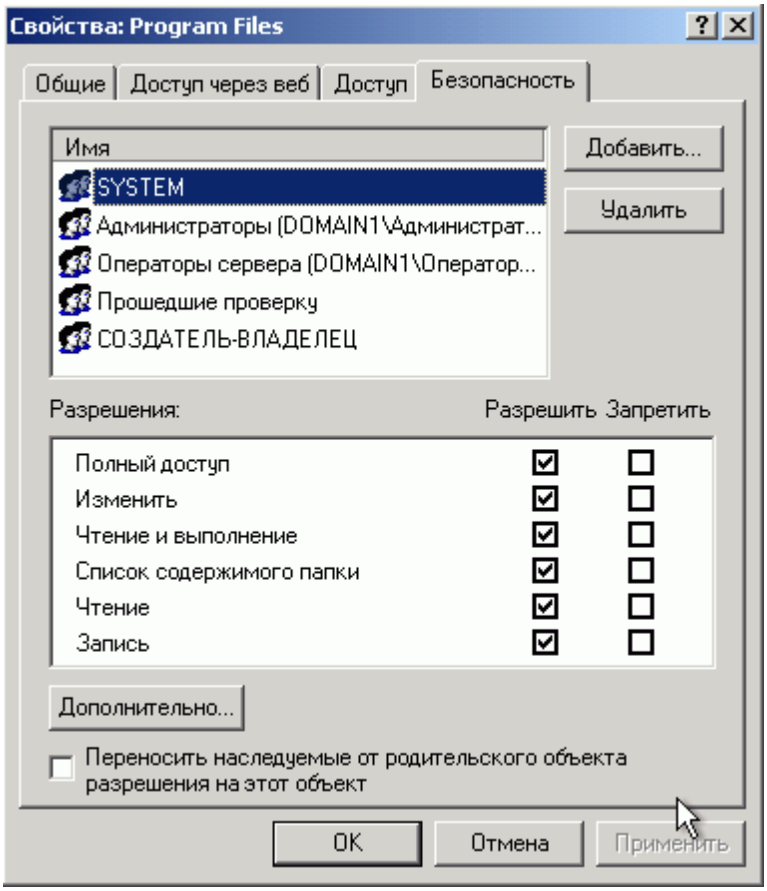
Чтение	Просматривать файлы и вложенные папки. Просматривать имя владельца папки, разрешения и атрибуты, такие как "Только чтение", "Скрытый", "Архивный" и "Системный"
Чтение и выполнение	Перемещаться по папкам для обращения к другим файлам и папкам, а также выполнять действия, предусмотренные в разрешениях на чтение и ознакомление со списком содержимого папки
Запись	Создавать в папке новые файлы и вложенные папки, изменять атрибуты папки и просматривать имя владельца папки и разрешения
Изменение	Удалять папку и выполнять действия, предусмотренные в разрешении на запись и в разрешении на чтение и выполнение
Полный доступ	Изменять разрешения, владельца, удалять вложенные папки и файлы и выполнять действия, предусмотренные во всех остальных разрешениях на доступ к папкам NTFS

Проверка разрешений на доступ к папке

Администратор назначает папке разрешения из вкладки **Безопасность** диалогового окна **Свойства** папки. В том же диалоговом окне можно просмотреть текущие разрешения на доступ к папке.

Чтобы просмотреть вкладку **Безопасность**, выполните следующие действия.

1. В проводнике Windows щелкните папку правой кнопкой мыши, выберите **Свойства**.
2. В диалоговом окне **Свойства** перейдите на вкладку **Безопасность**.



Вкладка **Безопасность** состоит из двух разделов - **Имя** и **Разрешения**. В разделе **Имя** показан список

пользователей и групп, имеющих разрешения на доступ к этой папке. В разделе **Разрешения** показан список разрешений, которые можно дать или в которых следует отказать пользователю или группе.

Общие папки

Чтобы дать нескольким пользователям доступ к одному и тому же ресурсу, например, папке, его необходимо сделать общим. Назначение папки в качестве общей означает, что эта папка будет доступна по сети одновременно для нескольких пользователей. Когда папка сделана общей, пользователи могут получать доступ ко всем ее файлам и вложенным папкам, если они обладают соответствующими разрешениями.

Делать общими можно только папки, но не отдельные файлы. Если многим пользователям требуется доступ к одному и тому же файлу, этот файл необходимо перенести в папку и сделать эту папку общей.

Обычно общие папки размещаются на файловом сервере, но их можно поместить и на любом компьютере сети. Можно хранить файлы в общих папках по категориям или по их функциям. Например, общие файлы данных можно поместить в одну общую папку, а общие файлы приложений - в другую.

Ниже приведены некоторые характеристики общих папок:

- В проводнике Windows общая папка показана в виде значка, изображающего руку, держащую папку.
- Разрешения даются только на папку целиком, но не на отдельные файлы или вложенные папки, содержащиеся в ней.
- Когда папка делается общей, то по умолчанию группе "Все" дается разрешение на полный доступ.
- Когда к общей папке добавляется пользователь, он по умолчанию получает разрешение на чтение.
- При копировании общей папки исходная папка остается общей, но ее копия общей папкой не является. При перемещении общей папки она перестает быть общей.

Уровень доступа к общей папке контролируется назначением этой папке разрешений. В следующей таблице перечислены разрешения на доступ к общей папке и задач, которые эти разрешения позволяют выполнять пользователям:

Разрешение на доступ к общей папке	**Позволяет пользователю**
Чтение	Просматривать имена папок, имена файлов, данные и атрибуты файлов, выполнять файлы приложений и изменять папки в пределах общей папки
Изменение	Создавать папки, добавлять файлы в папки, изменять данные в файлах, добавлять данные к файлам, изменять атрибуты файлов, удалять файлы и папки и выполнять действия, предусмотренные в разрешении на чтение
Полный доступ	Изменять разрешения на доступ к файлу, владение файлами и выполнять действия, предусмотренные в разрешении на изменение

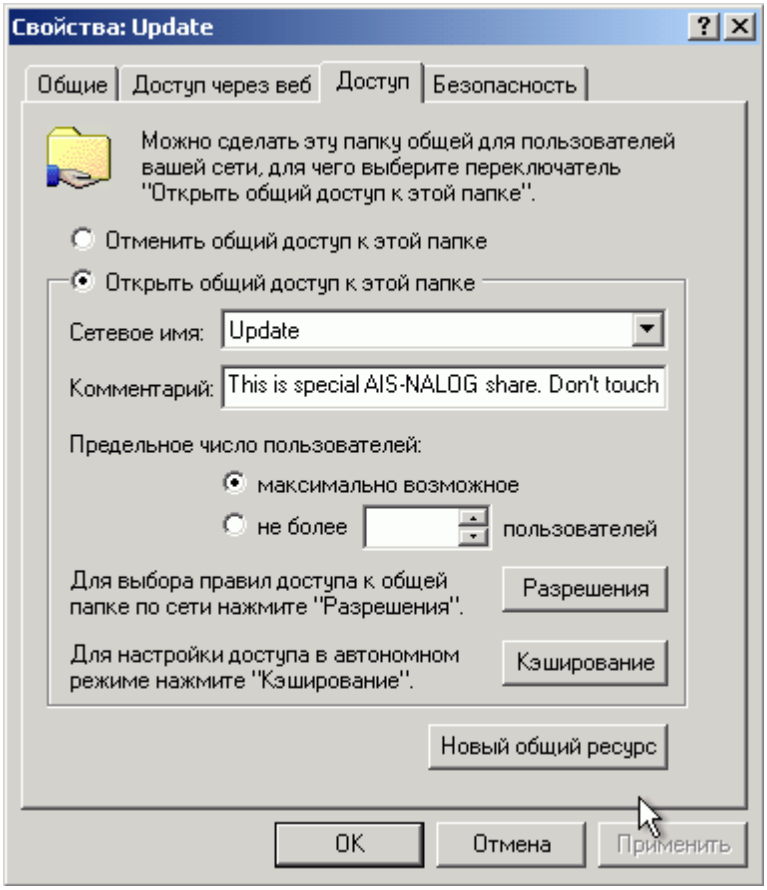
Разрешения на доступ к общей папке могут быть даны пользователям или же они могут быть отменены. Чтобы отказать в любом виде доступа к общей папке, отменяется разрешение на полный доступ.

Проверка разрешений на доступ к общей папке

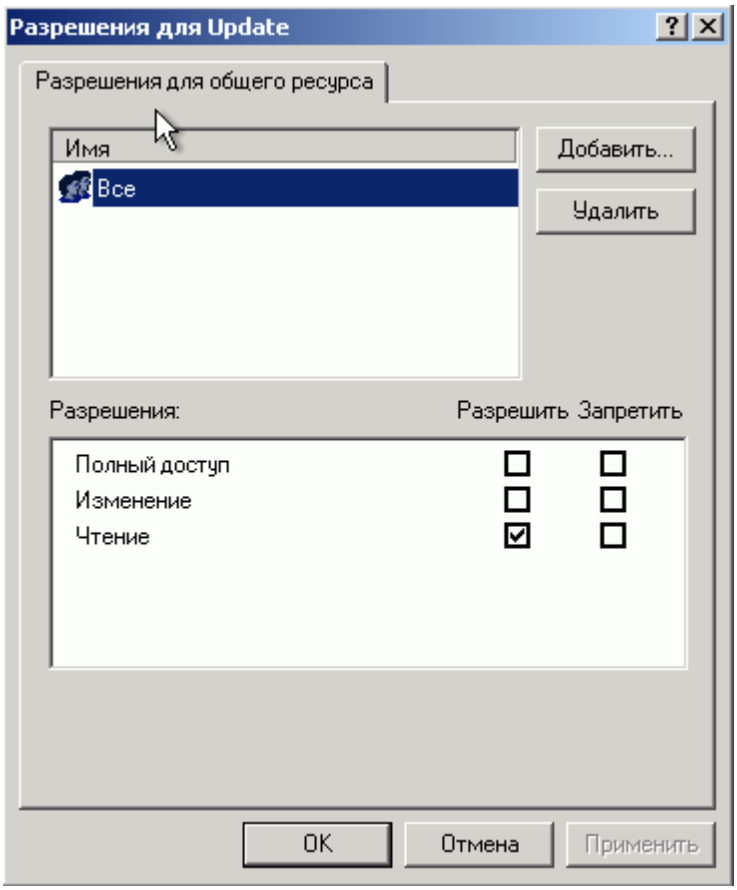
После создания общей папки администратор может назначить разрешения на доступ к этой общей папке пользователям или группам из диалогового окна "Разрешения" общей папки. В том же диалоговом окне можно просмотреть существующие разрешения на доступ к общей папке.

Чтобы проверить разрешения на доступ к общей папке, назначенные пользователям и группам, выполните следующие действия:

1. Щелкните общую папку правой кнопкой мыши в проводнике Windows.
2. Выберите команду **Свойства**.



3. На вкладке **Доступ** диалогового окна **Свойства** щелкните **Разрешения**.
4. Выберите учетную запись пользователя или группу, разрешения которой хотите просмотреть.



Для закрепления навыков по управлению доступом к файлам и общим папкам выполните упражнение Б.

Разрешения на доступ к принтерам

Разрешения на доступ к принтеру даются пользователям, не являющимся администраторами. Эти разрешения управляют действиями пользователей, связанными с печатью; с их помощью можно также ограничить доступ пользователей к определенным принтерам из соображений безопасности.

Уровни разрешений на доступ к принтеру

Разрешение на доступ к принтеру	Позволяет пользователю
Печать	Подключаться к принтеру, печатать и отменять печать своих документов
Управление документами	Подключаться к принтеру; приостанавливать, возобновлять, перезапускать и отменять печать всех документов
Управление принтерами	Выполнять все задачи, предусмотренные в разрешениях на печать и управление документами. Кроме того, это разрешение позволяет делать принтер общим ресурсом, изменять свойства принтера, удалять принтер и изменять разрешения на доступ к принтеру

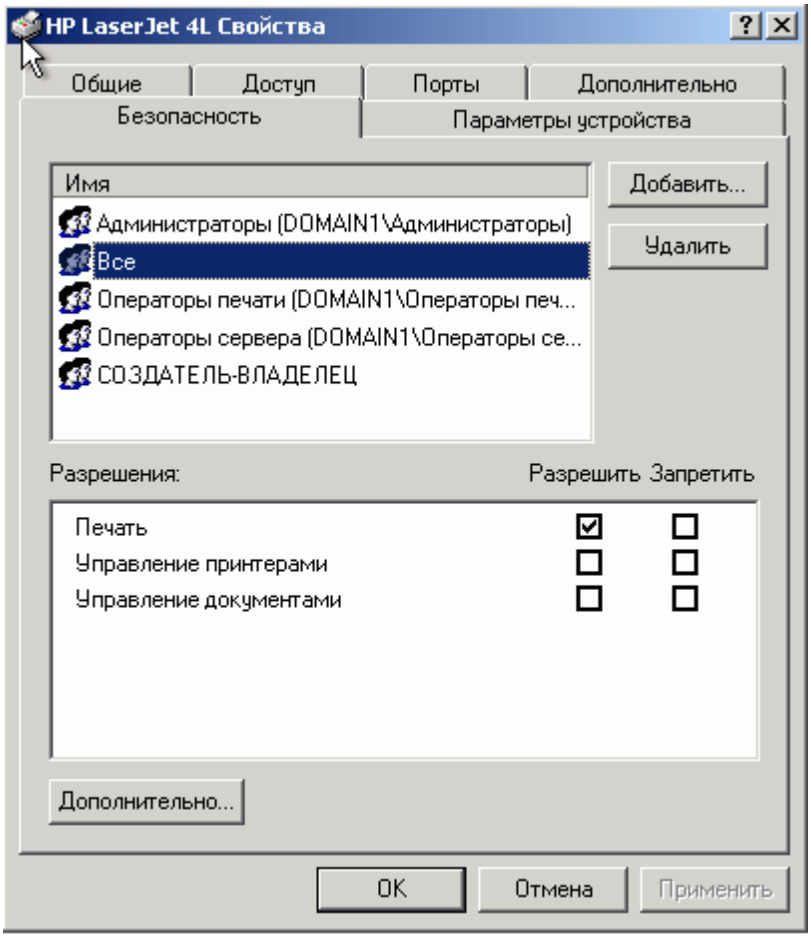
Проверка разрешений на доступ к принтеру

Назначать разрешения на доступ к принтеру можно отдельным пользователям или группам. По умолчанию операционная система Windows 2000 назначает разрешение на печать для каждого принтера встроенной группе "Все", тем самым давая всем пользователям возможность направлять

документы на любой принтер. Однако администратор может изменить эти разрешения, если есть необходимость ограничить доступ к принтеру определенным пользователям или группам. Например, администратор может разрешить использование цветного принтера только руководителям. В этом случае действующее по умолчанию разрешение группы "Все" можно снять и назначить разрешение исключительно группе "Начальники".

Чтобы просмотреть существующие разрешения на доступ к принтеру, выполните следующие действия:

1. В меню **Пуск** укажите команду **Найти** и выберите команду **Принтеры** для вывода диалогового окна **Поиск принтеров**.
2. В окне **Имя** вкладки **Принтеры** введите имя принтера и щелкните **Найти**.
3. Правой кнопкой мыши щелкните имя принтера и выберите **Свойства**.
4. В диалоговом окне **Свойства** перейдите на вкладку **Безопасность**. Здесь можно посмотреть существующие разрешения на доступ к принтеру для пользователей и групп.



Упражнение 2.Б: "Предоставление пользователям доступа к ресурсам"

Краткое описание

В этом упражнении Вы научитесь предоставлять пользователям доступ к файлам и папкам на жестком диске, а также к общим папкам.

Предварительные требования к выполнению упражнения

Выполнение упражнения 2.А

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.А по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. На **Рабочем столе** последовательно щелкните **Мой компьютер**, а затем **Локальный диск (C:)**.
3. Создайте папку ***Кадры***, щелкните на ней правой кнопкой и последовательно выберите **Свойства**, **Безопасность**.
4. Снимите флажок **Переносить наследуемые от родительского объекта разрешения на этот объект** и выберите в окне **Безопасность** пункт **Удалить**.
5. Нажмите **Добавить...**, в окне **Выбор: пользователи, компьютеры или группы** выберите группу ***Кадры*** и нажмите **Добавить**, **OK**.
6. В окне **Свойства: Кадры** убедитесь, что выбрана группа **Кадры**, предоставьте этой группе разрешение ***Изменить***.
7. Нажмите **Добавить...**, в окне **Выбор: пользователи, компьютеры или группы** выберите группу ***Прошедшие проверку*** и нажмите **Добавить**, **OK**.
8. В окне **Свойства: Кадры** убедитесь, что выбрана группа **Прошедшие проверку**, предоставьте этой группе разрешение ***Чтение и выполнение***.
9. Нажмите **Добавить...**, в окне **Выбор: пользователи, компьютеры или группы** выберите группу ***Администраторы*** и нажмите **Добавить**, **OK**.
10. В окне **Свойства: Кадры** убедитесь, что выбрана группа **Администраторы**, предоставьте этой группе разрешение ***Полный доступ***.
11. Перейдите на закладку **Доступ**, выберите флажок **Открыть общий доступ к этой папке** и впишите в поле **Сетевое имя** ***Kadry***.
12. Нажмите **Разрешения**, убедитесь, что выбрана группа **Все**, а затем предоставьте этой группе разрешение ***Изменение***.

Примечание. Если папка общего доступа расположена на файловой системе NTFS, не нужно

назначать на нее разрешения так же подробно, поскольку при сложении разрешений на файловую систему и на папку общего доступа выбираются самые ограничивающие разрешения. Рекомендуется задавать максимально жесткие разрешения на файловую систему, а на папку общего доступа - максимально допустимые разрешения.

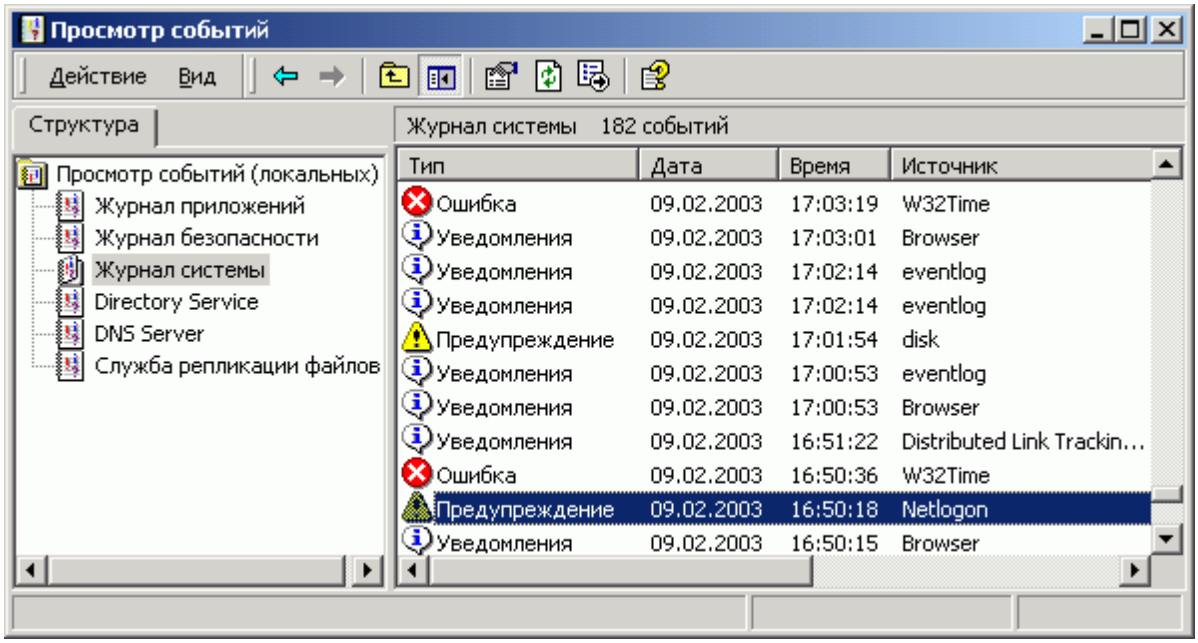
13. Нажмите **Добавить...**, в окне **Выбор: пользователи, компьютеры или группы** выберите группу ***Администраторы*** и нажмите **Добавить**, **ОК**.
14. В окне **Разрешения для Kadry** убедитесь, что выбрана группа **Администраторы**, предоставьте этой группе разрешение ***Полный доступ***.
15. Нажмите **ОК**, **ОК**.
16. Зайдите в папку **Кадры** и создайте текстовый документ с именем ***Кадровая политика.txt***. Щелкните файл правой кнопкой и последовательно выберите **Свойства**, **Безопасность**.
17. Проверьте, что файл унаследовал установленные на папку разрешения.

Занятие 4: "Наблюдение за работой сети"

При наблюдении за работой сети мы можем контролировать не только работоспособность ключевых устройств сети, но и их производительность. Для контроля за состоянием серверов и рабочих станций под управлением Windows 2000 используется инструмент **"Просмотр событий"**, а для оценки производительности - инструменты "Диспетчер задач" и "Производительность".

Инструмент "Просмотр событий"

Инструмент "Просмотр событий" объединяет информацию об оборудовании, программном обеспечении, проблемах в системе, а также о событиях системы безопасности. ***Событием*** называется любое значимое событие, происходящее с приложением или с операционной системой. Каждый раз, когда происходит какое-либо событие, операционная система Windows 2000 записывает информацию о нем в журнал. Таким образом, просматривая записи в окне "Просмотр событий", можно следить за состоянием системы.



Чтобы использовать инструмент "Просмотр событий", на **панели управления** откройте раздел **Администрирование**, а затем **Просмотр событий**.

Типы событий

Инструмент "Просмотр событий" отображает события четырех типов:

- **Ошибка** - указывает на серьезную ошибку, например, на потерю данных или сбой в системе.
- **Предупреждение** - указывает на вероятность возникновения ошибки.
- **Уведомление** - описывает действие, успешно выполненное приложением, драйвером или службой.
- **Аудит** - отображает сообщения об успешных и неуспешных попытках доступа к контролируемому ресурсу.

Инструмент "Просмотр событий" записывает эти события в журналы. В зависимости от того, какие

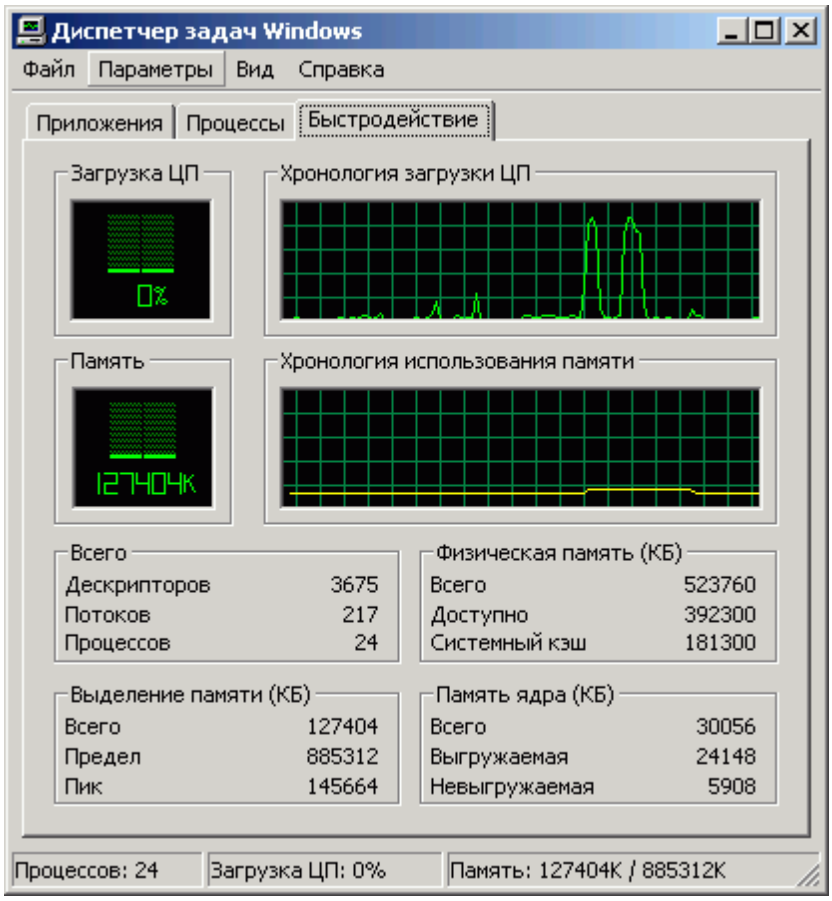
дополнительные компоненты установлены в системе, создаются различные типы журналов событий. Основные журналы событий - **Журнал приложений**, **Журнал системы** и **Журнал безопасности**.

- В **Журнале приложений** содержатся сообщения о событиях, записанных приложениями. Например, приложение базы данных может записать в этот журнал сведения об ошибке, произошедшей при работе с файлом. В этом журнале содержатся сообщения о событиях типа **Ошибка**, **Предупреждение** и **Уведомление**.
- В **Журнале системы** содержатся сообщения о событиях, записанных системными компонентами Windows 2000. Например, в журнал системы записываются сообщения о неудачной загрузке компонентов системы при запуске. В этом журнале содержался сообщения о событиях типа **Ошибка**, **Предупреждение** и **Уведомление**.
- В **Журнале безопасности** содержатся сообщения только о **событиях аудита**, включая удачные и неудачные попытки входа, а также сообщения о событиях, связанных с использованием ресурсов, например, с созданием, открытием и удалением файлов.

Диспетчер задач Windows

Наблюдение за производительностью системы является неотъемлемой частью обслуживания и администрирования компьютера на базе Windows 2000. Диспетчер задач Windows представляет собой простое средство, позволяющее следить за производительностью компьютера и просматривать общую информацию о системе.

Диспетчер задач Windows выдает информацию о производительности компьютера, а также о текущих процессах и выполняемых приложениях. С помощью диспетчера задач Windows можно запускать и закрывать приложения, завершать процессы, а также просматривать в реальном времени статистику работы компьютера.



Чтобы использовать диспетчер задач Windows, щелкните правой кнопкой мыши на свободное место на панели задач и выберите **Диспетчер задач** или нажмите комбинацию клавиш **Ctrl+Shift+Esc**.

Информацию, отображаемую диспетчером задач Windows, можно просмотреть на трех вкладках:

Приложения, **Процессы** и **Быстродействие**.

- На вкладке **Приложения** показано состояние приложений, запущенных на компьютере. С помощью этой вкладки можно запустить, закрыть приложение или переключиться на него.
- На вкладке **Процессы** отображены сведения о текущих процессах в системе. Процессом может быть приложение (например, Microsoft Windows Explorer) или служба (например, журнал событий).
- На вкладке **Быстродействие** динамически отображается информация о работе компьютера, в том числе сведения об использовании процессора и памяти.

Инструмент "Производительность"

Инструмент "Производительность" является расширенным вариантом диспетчера задач Windows и предлагает более подробную информацию. С помощью сведений, предоставляемых этим средством, можно следить за производительностью локального компьютера или компьютеров в сети.

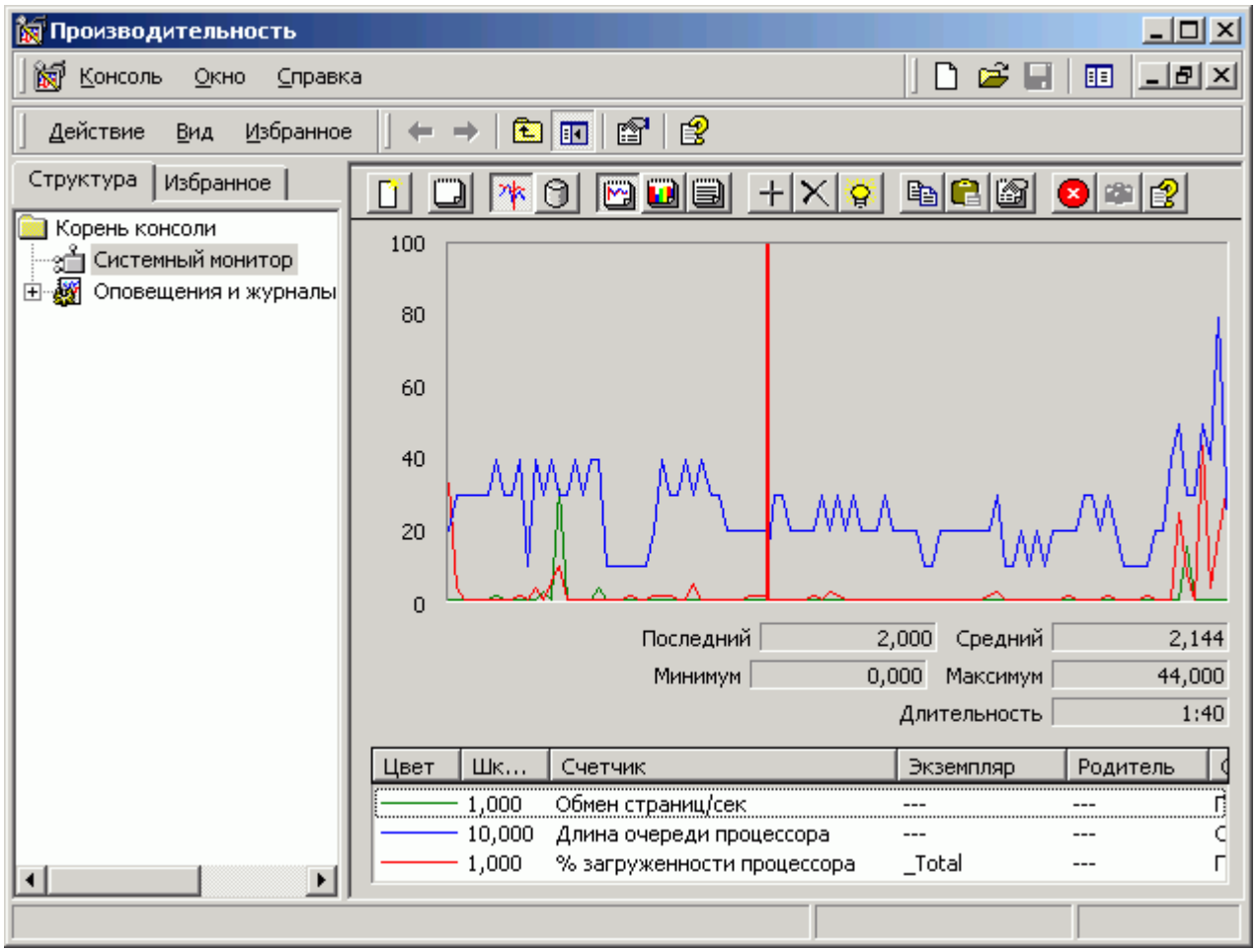
Данные, предоставляемые инструментом "Производительность", можно использовать в следующих целях:

- анализ изменений рабочей нагрузки и оценка влияния этой нагрузки на ресурсы системы;
- наблюдение за изменениями рабочей нагрузки и тенденциями изменения нагрузки с целью планирования обновления системы;
- оценка изменений системной конфигурации посредством контроля результатов;
- диагностика проблем и выявление компонентов или процессов, нуждающихся в улучшении.

Чтобы запустить инструмент "Производительность", на **панели управления** последовательно откройте **Администрирование**, затем **Системный монитор**.

Инструмент "Производительность" состоит из двух служебных программ: "Системный монитор" и "Оповещения и журналы производительности". Эти служебные программы предоставляют подробные данные о ресурсах, используемых отдельными компонентами операционной системы, а также приложениями и службами, выполняемыми в системе.

"Системный монитор"



С помощью инструмента "Системный монитор" можно:

- собирать информацию о производительности компьютера и сравнивать ее с данными о производительности других компьютеров в сети:
- собирать и просматривать данные, полученные с локального компьютера или с нескольких удаленных компьютеров в сети;
- просматривать данные, собираемые в текущий момент или полученные ранее и сохраненные в файле журнала;
- представлять данные в виде графика, гистограммы или отчета, которые при необходимости можно распечатать; график является стандартным представлением и предлагает наиболее широкий выбор необязательных настроек;
- создавать веб-документ на основе представлений с информацией о производительности;
- создавать конфигурации наблюдения для многократного использования, которые затем можно устанавливать на других компьютерах.

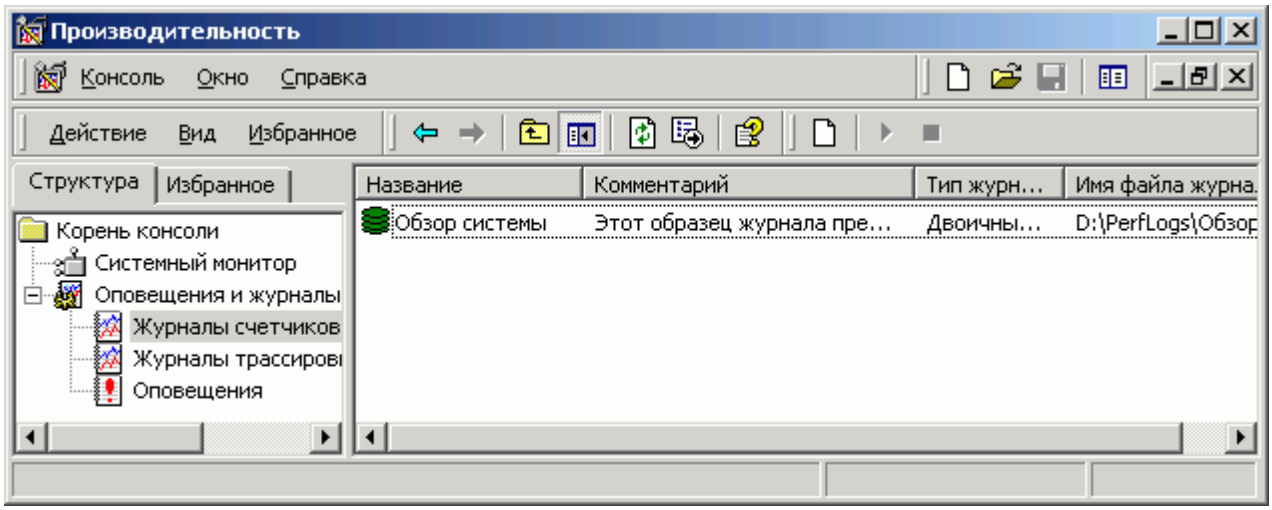
Для того, чтобы определить производительность и текущее состояние компьютера, необходимо оценить нагрузку на три важнейших компонента:

1. **Процессор**. Для определения степени загрузки процессора используется счетчик **% загруженности процессора** из объекта **Процессор**. Если загрузка процессора стабильно превышает **75%**, следовательно, он перегружен и нужно производить модернизацию процессора или переносить часть задач на другие компьютеры.
2. **Память**. Для определения степени загрузки оперативной памяти используется счетчик **Обмен страниц/сек** из объекта **Память**. Если этот параметр стабильно превышает **20**, то системе не хватает оперативной памяти и она вынуждена постоянно обмениваться данными с виртуальной памятью (файл подкачки) на жестком диске. Тогда необходимо увеличить объем оперативной памяти или перенести часть задач на другие компьютеры.
3. **Жесткий диск**. Для определения степени загрузки жесткого диска используется счетчик **% активности диска** из объекта **Физический диск**. При стабильном превышении загрузки жесткого диска выше **50%**, диск считается перегруженным. В этом случае нужно обновить

жесткий диск, или добавить еще один диск и разнести нагрузку между ними, или переносить часть задач на другие компьютеры.

Чтобы выбрать счетчики, правой кнопкой мыши щелкните на графике и выберите **Добавить счетчики...**. Выберите объект и счетчик и нажмите **Добавить**, чтобы системный монитор начал наблюдение за выбранным счетчиком. Используйте комбинацию клавиш **CTRL+H** или пункт панели управления **Выделить**, чтобы точнее следить за нужным счетчиком.

"Оповещения и журналы производительности"



Инструмент "Оповещения и журналы производительности":

- устанавливает интервалы выборки для сбора информации об аппаратных ресурсах и системных службах;
- собирает информацию в течение определенного периода времени и архивирует ее;
- поддерживает настройку оповещений о достижении определенного порога.

Для закрепления навыков по использованию средств наблюдения выполните упражнение В.

Упражнение 2.B: "Наблюдение за рабочей станцией"

Краткое описание

В этом упражнении Вы научитесь использовать инструменты "Диспетчер задач" и "Системный монитор" для контроля за состоянием рабочей станции.

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.A по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. Нажмите клавиши **CTRL+SHIFT+ESCAPE**, чтобы вызвать **Диспетчер задач**.
3. Перейдите на вкладку **Приложения**. Просмотрите, какие программы сейчас выполняются.
4. Перейдите на вкладку **Процессы**. Просмотрите, какие пользовательские и системные процессы сейчас выполняются. Отсортируйте их сначала по колонке **ЦП**, чтобы узнать, какие процессы сейчас нагружают систему, а затем по колонке **Память**, чтобы определить, какие процессы занимают больше всего памяти.
5. Перейдите на вкладку **Быстродействие**. Просмотрите, какова нагрузка на процессор и сколько памяти используется.
6. Чтобы больше узнать о загруженности системы, запустите инструмент **Системный монитор**. Для этого на **панели управления** последовательно откройте **Администрирование**, затем **Системный монитор**
7. Правой кнопкой щелкните график и выберите **Добавить счетчики...**.
8. Выберите в объекте **Процессор** счетчик **% загруженности процессора** и нажмите **Добавить**. Повторите операцию для счетчика **Обмен страниц/сек** из объекта **Память** и счетчика **% активности диска** из объекта **Физический диск**.
9. Нажмите **Закрыть** и запустите игру **Пинбол**, чтобы сэмулировать нагрузку на рабочую станцию. Для этого последовательно выберите **Пуск**, **Программы**, **Стандартные**, **Игры**, **Пинбол**.
10. Не начиная игру, выйдите из приложения и посмотрите на график, чтобы оценить, насколько велика была нагрузка в момент запуска игры. Критерии перегрузки описаны в занятии 4
11. Нажмите **CTRL+H**, чтобы выделить активный счетчик. Это позволит точнее видеть данные выделенного счетчика.

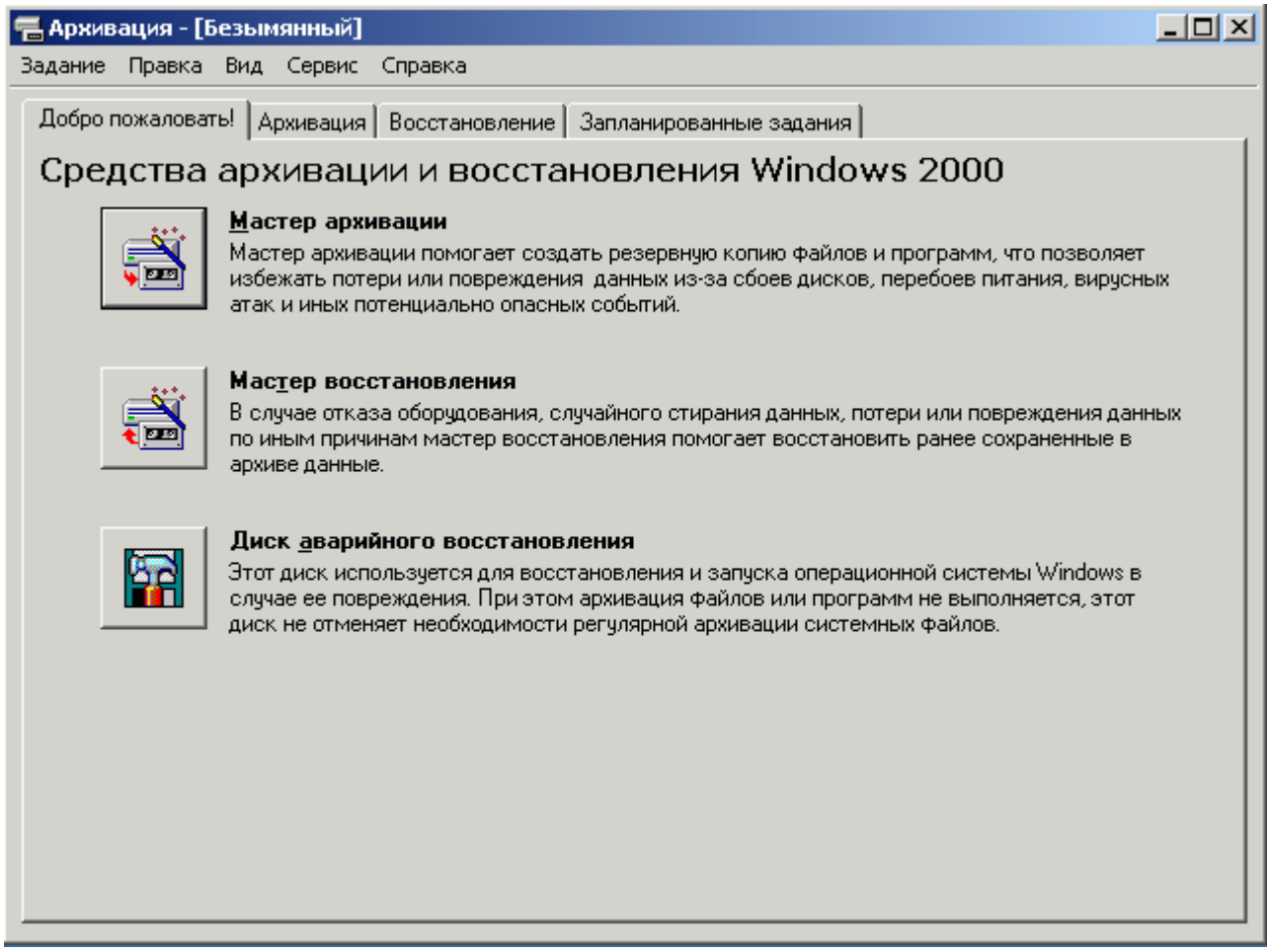
Занятие 5: "Архивирование и восстановление данных"

Цель любого задания архивации заключается в том, чтобы обеспечить эффективное восстановление данных, потерянных в результате сбоя. Систематически делая архивные копии данных на жестких дисках сервера и клиентского компьютера, можно предотвратить потерю данных, к которой приводят отказы дисков, сбои питания, проникновение вирусов и другие инциденты. Если регулярно выполнять задания архивации в соответствии с тщательно продуманным расписанием, то можно будет всегда восстановить потерянные данные, независимо от того, что повреждено - один файл или весь жесткий диск.

Инструмент "Архивация данных"

В состав системы Windows 2000 входит инструмент "Архивация данных", которая позволяет выполнять следующие операции:

- архивировать файлы и папки;
- архивировать данные о состоянии системы;
- планировать проведение архивации по расписанию;
- восстанавливать файлы и папки.



Чтобы запустить инструмент "Архивация данных", последовательно нажмите **Пуск**, **Программы**, **Стандартные**, **Служебные**, **Архивация данных**.

Разрешения и права пользователей

Чтобы успешно проводить архивацию и восстановление данных на компьютере, работающем под управлением системы Windows 2000, необходимо обладать соответствующими разрешениями и правами пользователя, как описано ниже:

- Все пользователи могут архивировать свои собственные файлы и папки. Они могут также архивировать файлы, в отношении которых имеют разрешение на чтение.
- Все пользователи могут восстанавливать файлы и папки, в отношении которых они имеют разрешение на запись.
- Члены групп "Администраторы", "Операторы архива" и "Операторы сервера" могут архивировать и восстанавливать все файлы, независимо от назначенных им разрешений. По умолчанию члены этих групп обладают пользовательскими правами "Архивирование файлов и каталогов" и "Восстановление файлов и каталогов".

Архивация данных о состоянии системы

С помощью программы архивации можно делать архивные копии данных о состоянии системы. Если данные о состоянии системы на каком-либо компьютере были сархивированы, а затем произошел сбой системы, можно восстановить состояние компьютера, используя исходный компакт-диск Windows 2000 и данные о состоянии системы. Данные о состоянии системы содержат информацию, необходимую для восстановления того состояния операционной системы, в котором она пребывала до возникновения сбоя.

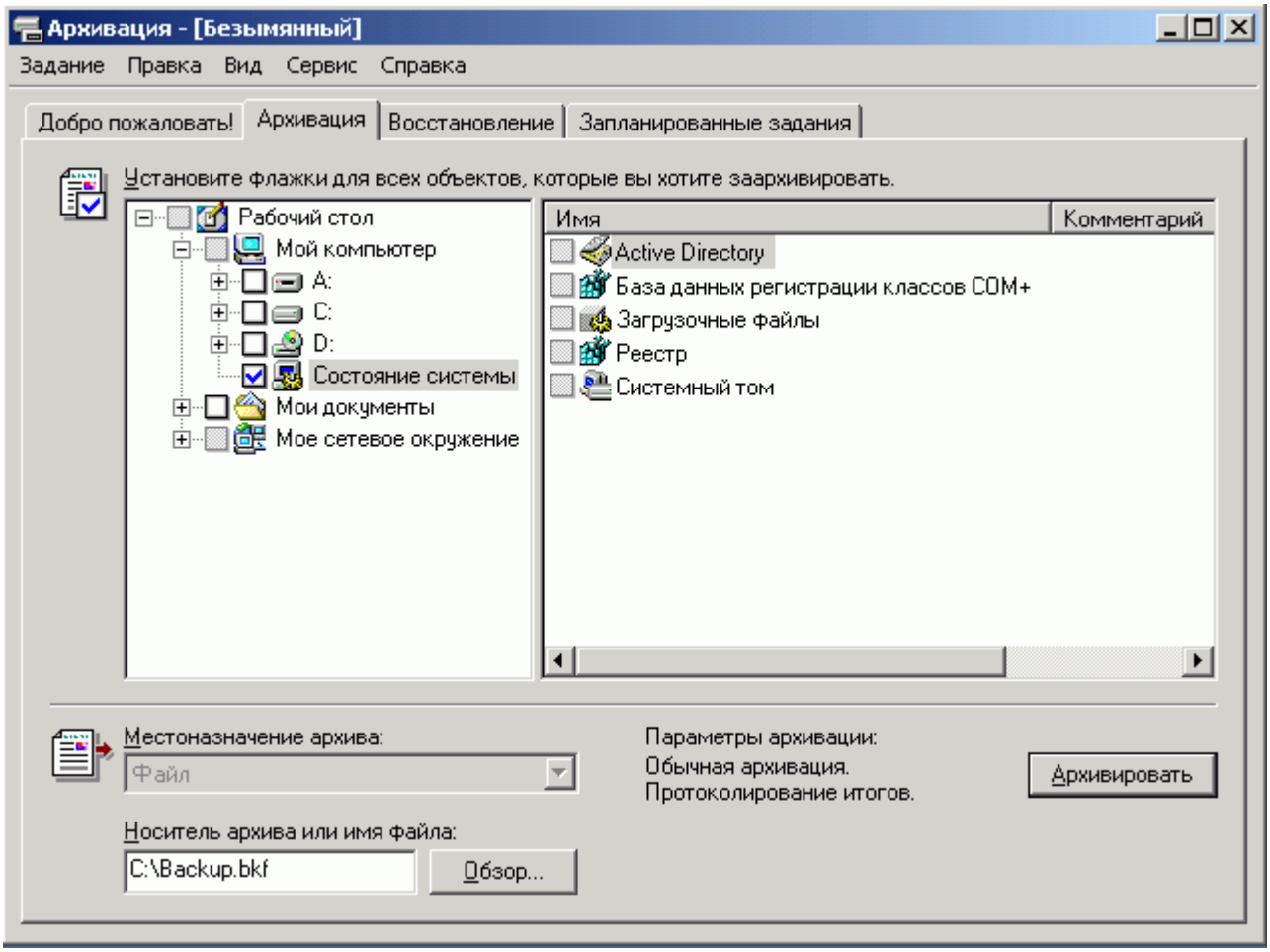
Эти данные включают следующие компоненты:

- реестр;
- база данных службы "Службы компонентов";
- файлы запуска системы;
- база данных службы "Службы сертификации";
- база данных службы каталогов Active Directory;
- папка Sysvol.

В системе Windows 2000 Professional данные о состоянии системы включают реестр, базу данных регистрации служб компонентов и файлы запуска системы. В операционных системах Windows 2000 Server данные о состоянии системы включают, помимо этого, базу данных служб сертификации (если компьютер является сервером сертификатов), каталог Active Directory и папку Sysvol (если компьютер является контроллером домена).

Архивация данных о состоянии системы на локальном компьютере осуществляется одним из трех способов:

- В окне мастера архивации на странице **Что следует архивировать** установите переключатель **Архивировать только данные состояния системы**.
- В окне мастера архивации на странице **Элементы для архивации** разверните элемент **Мой компьютер** и установите флажок слева от элемента **Состояние системы**.
- В окне программы архивации на вкладке **Архивация** разверните элемент **Мой компьютер** и установите флажок слева от элемента **Состояние системы**.



Архивация по расписанию

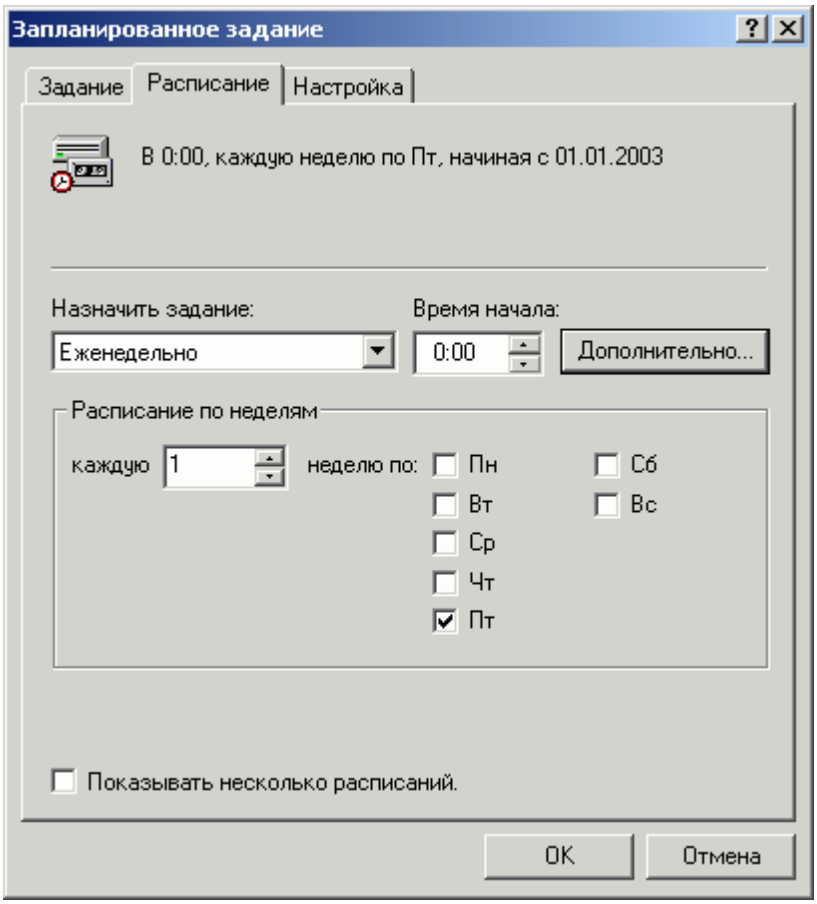
Программа архивации данных интегрирована со службой "Планировщик заданий". Поэтому с помощью программы архивации можно также планировать задания архивации. Можно составить расписание так, чтобы архивация выполнялась с регулярными интервалами или во время периодов пониженной активности в сети. Планировать архивацию можно двумя способами: во время составления задания архивации или на вкладке **Запланированные задания** в окне программы архивации.

Чтобы создать плановую архивацию в процессе составления задания архивации, выполните следующие действия.

1. На странице **Завершите работу мастера архивации** нажмите **Дополнительно**.
2. На странице **Когда архивировать** установите переключатель **Позже**, введите имя задания и нажмите **Установить расписание**.
3. В диалоговом окне **Запланированное задание** задайте требуемые параметры (такие, как частота и время начала архивации) и нажмите **OK**.

Чтобы создать плановую архивацию на вкладке **Запланированные задания** в окне программы архивации, выполните следующие действия.

1. На **Запланированные задания** окна **Архивация** дважды щелкните день, когда следует запустить плановую архивацию.
2. Введите нужные для мастера архивации данные. Покажите, как планировать задание архивации.

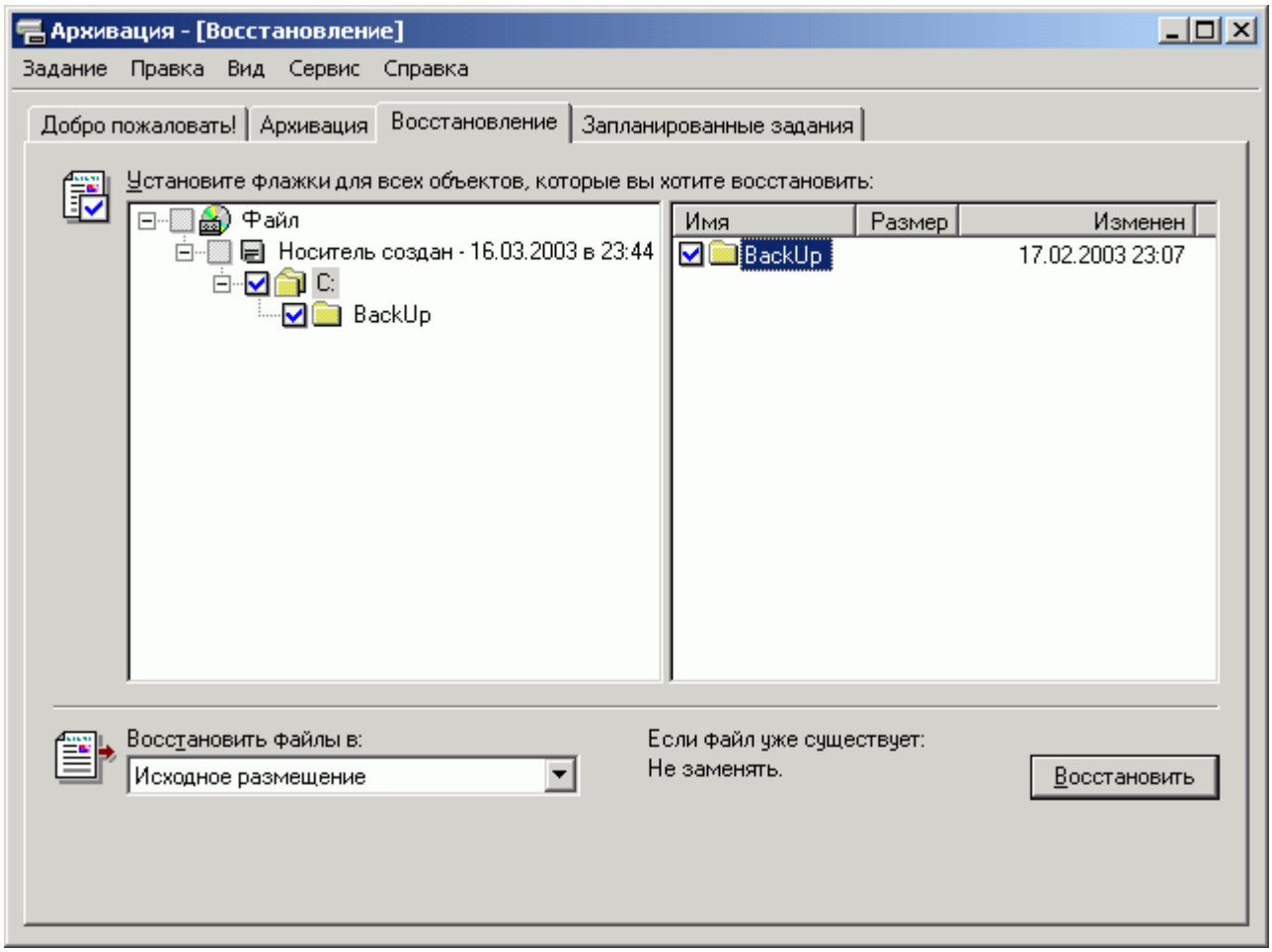


Восстановление файлов и папок

Программу архивации данных можно использовать и для восстановления файлов и папок после потери данных. В состав программы архивации входит **Мастер восстановления**, под руководством которого пользователь последовательно выполняет все шаги процедуры восстановления. Программа архивации позволяет также восстанавливать файлы и папки вручную, без помощи мастера.

Для восстановления файлов и папок необходимо задать следующее:

- Папки или файлы, подлежащие восстановлению.
- Место восстановления. Файлы можно восстановить в их первоначальном месте, в другом месте или в отдельной папке.
- Параметры восстановления: например, нужно ли замещать уцелевшие файлы архивными копиями.



Советы и рекомендации

- **Разработайте и проверьте на практике систему архивации и восстановления**. Хорошая система гарантирует быстрое восстановление данных в случае их утери.
- **Обучите соответствующих сотрудников**. В сетях с минимальной или средней защитой наделите правами архивации одного пользователя, а правами восстановления — другого. Обучите сотрудников с правами на восстановление выполнять все задачи восстановления в случае отсутствия администратора. В сетях с высокой защитой восстановление файлов должно выполняться только администраторами.
- **Архивируйте тома целиком**. Архивация всего тома обеспечивает готовность к негативным событиям типа поломки диска. Операция восстановления всего тома за один прием является более эффективной.
- **Архивируйте службы каталогов**. Всегда выполняйте архивацию базы данных служб каталогов контроллера домена для предотвращения потери данных учетных записей пользователей и сведений о безопасности.
- **Создавайте журнал архивации**. Для каждой архивации создавайте и печатайте журналы архивации. Для упрощения нахождения каких-либо файлов храните книгу журналов. Журналы архивации, которые можно напечатать или просмотреть в любом текстовом редакторе, бывают полезны при восстановлении данных. Кроме того, если лента, содержащая каталог архива, повреждена, напечатанный журнал поможет найти требуемый файл.
- **Храните копии**. Храните три копии носителя. По крайней мере одну копию храните в надежном месте вне организации.
- **Выполняйте пробное восстановление**. Периодически выполняйте пробное восстановление для проверки правильности архивации файлов. Пробное восстановление может помочь обнаружить неполадки оборудования, незаметные при программной проверке.
- **Обеспечивайте безопасность устройств и носителей**. Обеспечивайте безопасность и устройств хранения данных, и носителей архива. Восстановление данных с утерянного носителя возможно каким-либо пользователем на другом сервере, администратором которого он является.

Занятие 6: "Обслуживание жестких дисков"

Одной из задач администрирования компьютера является управление дисками. Знание средств, используемых для настройки и управления дисками и возможностей, предоставляемых системой Windows 2000, позволит вам лучше управлять дисковыми накопителями.

Базовые и динамические диски

Windows 2000 поддерживает базовые и динамические диски. При установке операционной системы Windows 2000 жесткий диск автоматически будет инициализирован в качестве базового. После завершения установки можно использовать мастер обновления для преобразования этого диска в динамический. В одной системе можно использовать как базовые, так и динамические диски, но тома, состоящие из нескольких дисков, например зеркальные тома, должны использовать только один тип дисков.

Понятие ***базовый диск*** в Windows 2000 соответствует схеме организации разделов системы MS-DOS, когда таблица разделов размещается в начале диска и максимальное число записей в ней равно четырем. На базовом диске можно создать не более 4 основных разделов (с которых можно загружаться), либо 3 основных и 1 дополнительный раздел (загрузиться с него нельзя, но у него есть своя внутренняя таблица разделов, которая и используется для дальнейшего разбиения раздела на логические диски). Новые или пустые диски можно инициализировать в качестве базовых или динамических в процессе установки. Обратите внимание, что в Windows 2000 на базовых дисках невозможно создавать составные, чередующиеся, зеркальные и RAID-5 тома; расширять тома и наборы томов или вносить изменения на диск без перезапуска компьютера. Все эти операции выполняются только на динамических дисках.

Понятие ***динамический диск*** в Windows 2000 соответствует новой схеме организации разделов на физическом диске, когда таблица разделов размещается в конце диске и число записей в ней практически неограничено. Отсюда и другая терминология - динамические диски содержат не разделы или логические диски, а динамические тома. Динамические диски доступны только в Windows 2000/XP.

Для базовых и динамических дисков можно выполнять следующие действия:

- проверять свойства диска, такие как емкость, доступное свободное место и текущее состояние;
- просматривать свойства тома и раздела, такие как размер, назначенную букву диска, метку, тип и файловую систему;
- задавать буквы для томов или разделов диска и для дисковода для компакт-дисков;
- открывать общий доступ к диску и устанавливать параметры безопасности для томов и разделов;
- обновлять базовый диск до динамического или преобразовывать динамический диск в базовый.

Особенности динамических дисков

С динамическими дисками можно выполнять следующие операции:

- создавать или удалять простые, составные, чередующиеся, зеркальные и RAID-5 тома
- расширять простые или составные тома
- удалять зеркало из зеркального тома или разделять зеркальный том на два тома

- восстанавливать зеркальные тома или тома RAID-5
- реактивизировать отсутствующий или неподключенный диск

Динамические диски разбиваются на тома.

Том - это логическая часть жесткого диска, которой назначена буква диска или точка подключения. Тома можно создавать только на динамических дисках.

Простой том - занимает дисковое пространство только на одном диске, причем только на динамическом диске.

Составной том включает дисковое пространство двух или большего числа дисков (вплоть до 32-х дисков). При записи данных на составной том сначала заполняется часть составного тома, находящаяся на первом диске, а затем данные записываются на следующий диск тома. В случае неисправности одного из дисков составного тома теряются все данные, хранившиеся на этом диске. Составной том позволяет объединять дисковую память, однако не повышает быстродействие диска. Составной том создается только на динамическом диске.

Чередующийся том (***RAID0***) - объединяет участки свободного места двух или большего числа дисков (вплоть до 32 жестких дисков) в один том. При записи данных на чередующийся том, они разбиваются на 64-килобайтные блоки и равномерно распределяются по всем дискам массива. Такой процесс распределения данных по набору дисков повышает быстродействие диска, однако не обеспечивает отказоустойчивость. Чередующийся том создается только на динамическом диске.

Зеркальный том (***RAID1***) - это две идентичные копии простого тома, каждая из которых хранится на отдельном жестком диске. Использование зеркальных томов обеспечивает отказоустойчивость в случае неисправности жесткого диска. Он создается только на динамическом диске.

Том RAID-5 - это отказоустойчивый чередующийся том. Система Windows 2000 добавляет на каждый диск тома блок четности. Сами данные и информация об их четности размещаются так, чтобы они всегда оказывались на разных дисках. Для каждого блока данных на диске имеется полоса блока четности. Система Windows 2000 использует информацию о четности в этих полосах для восстановления данных в случае неисправности жесткого диска. Тома RAID-5 требуют использования не менее трех жестких дисков и создаются только на динамическом диске.

Особенности базовых дисков

С базовыми дисками можно выполнять следующие операции:

- создавать и удалять основные и дополнительные разделы
- создавать и удалять логические диски в пределах дополнительного раздела
- форматировать раздел и пометить его в качестве активного
- удалять наборы томов, чередующиеся наборы томов (с четностью и без) и зеркальные наборы (созданные до обновления с Windows NT 4.0 до Windows 2000)
- разделять зеркальный набор
- восстанавливать зеркальный набор или чередующийся набор с четностью

Базовые диски разбиваются на разделы

Раздел - это логическая часть жесткого диска, которой назначается буква диска. Создавать разделы можно только на базовом диске. Разделы бывают основными и дополнительными.

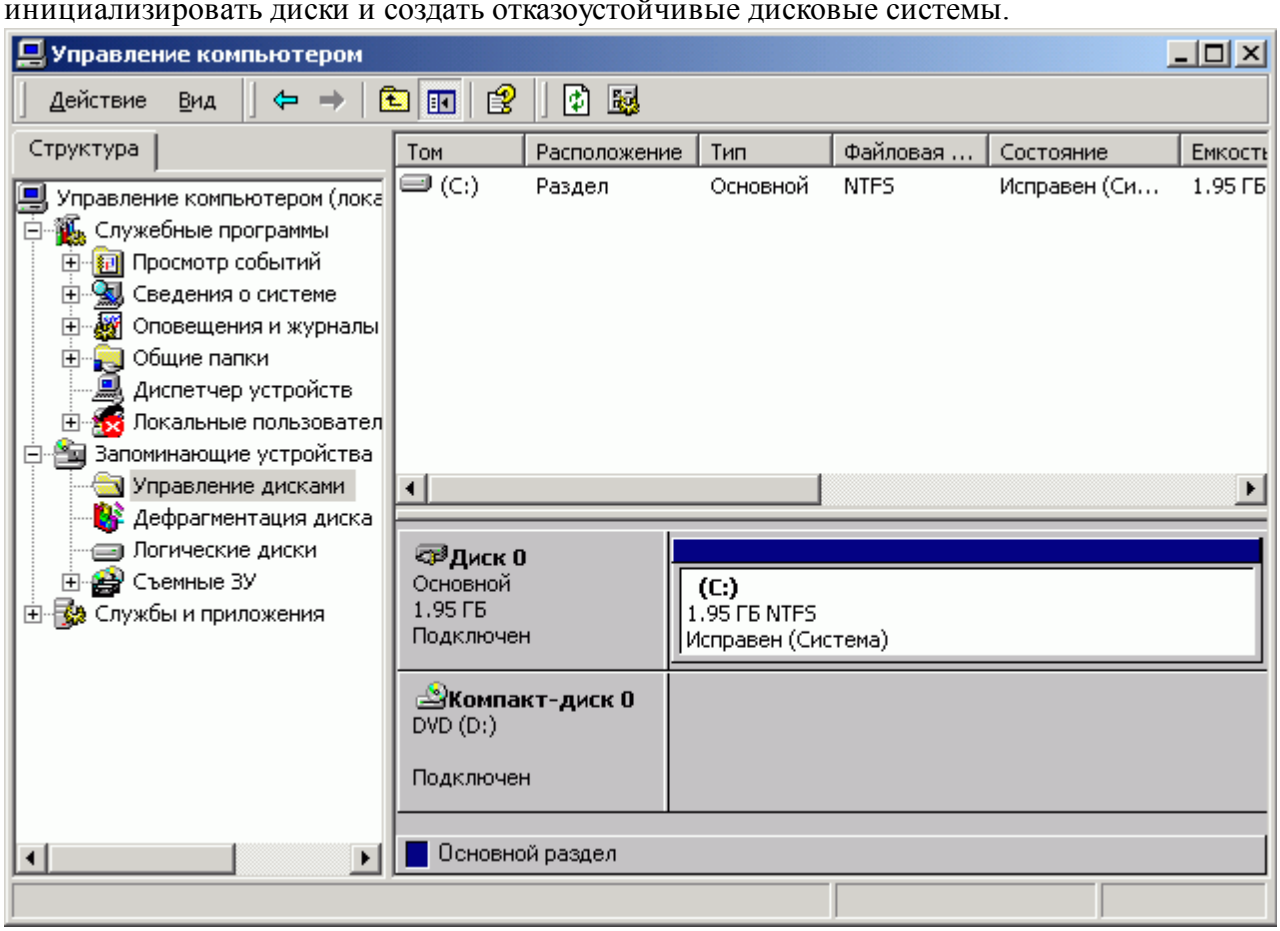
Основной раздел - это часть используемого места на диске, создаваемая из имеющегося на диске незанятого места. Каждому разделу назначается буква диска.

Дополнительный раздел - это часть используемого места на диске, создаваемая из имеющегося на диске незанятого места в том случае, если на базовом диске требуется создать более четырех областей хранения. Дополнительный раздел можно разделить на логические диски. Дополнительному разделу буква диска не назначается, они присваиваются только находящимся на нем логическим дискам.

Логический диск - это часть дополнительного раздела. Логический диск форматируется, и ему назначается буква диска. Логический диск не может занимать несколько физических дисков.

Управление дисками

Для управления жесткими дисками, томами или разделами, существует инструмент "Управление дисками". С его помощью можно создать тома, отформатировать их в необходимые файловые системы, инициализировать диски и создать отказоустойчивые дисковые системы.



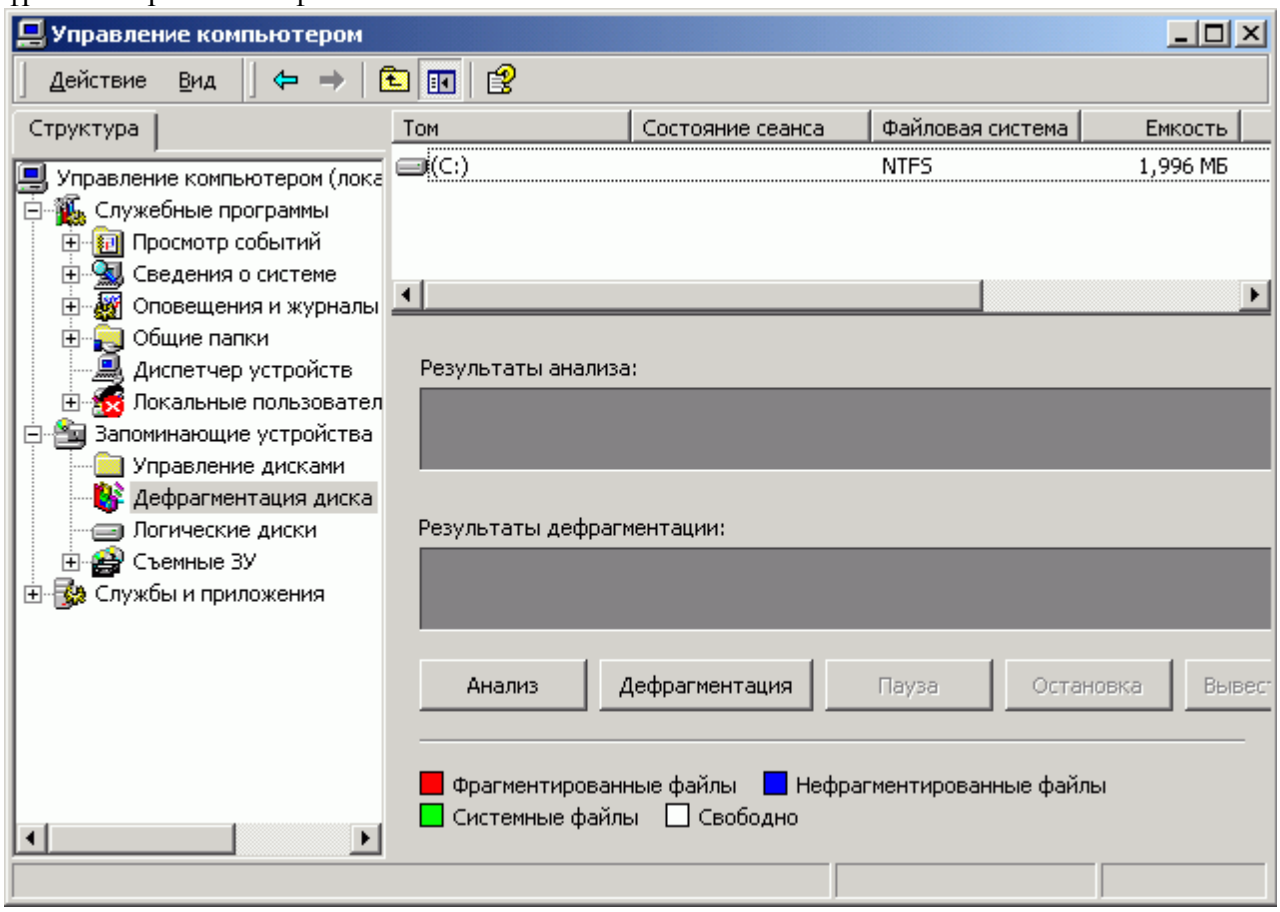
Чтобы запустить инструмент "Управление дисками", нажмите **Пуск**, выберите **Программы**, **Администрирование**, а затем **Управление компьютером**. В окне **Управление компьютером** выберите **Управление дисками**.

Дефрагментация диска

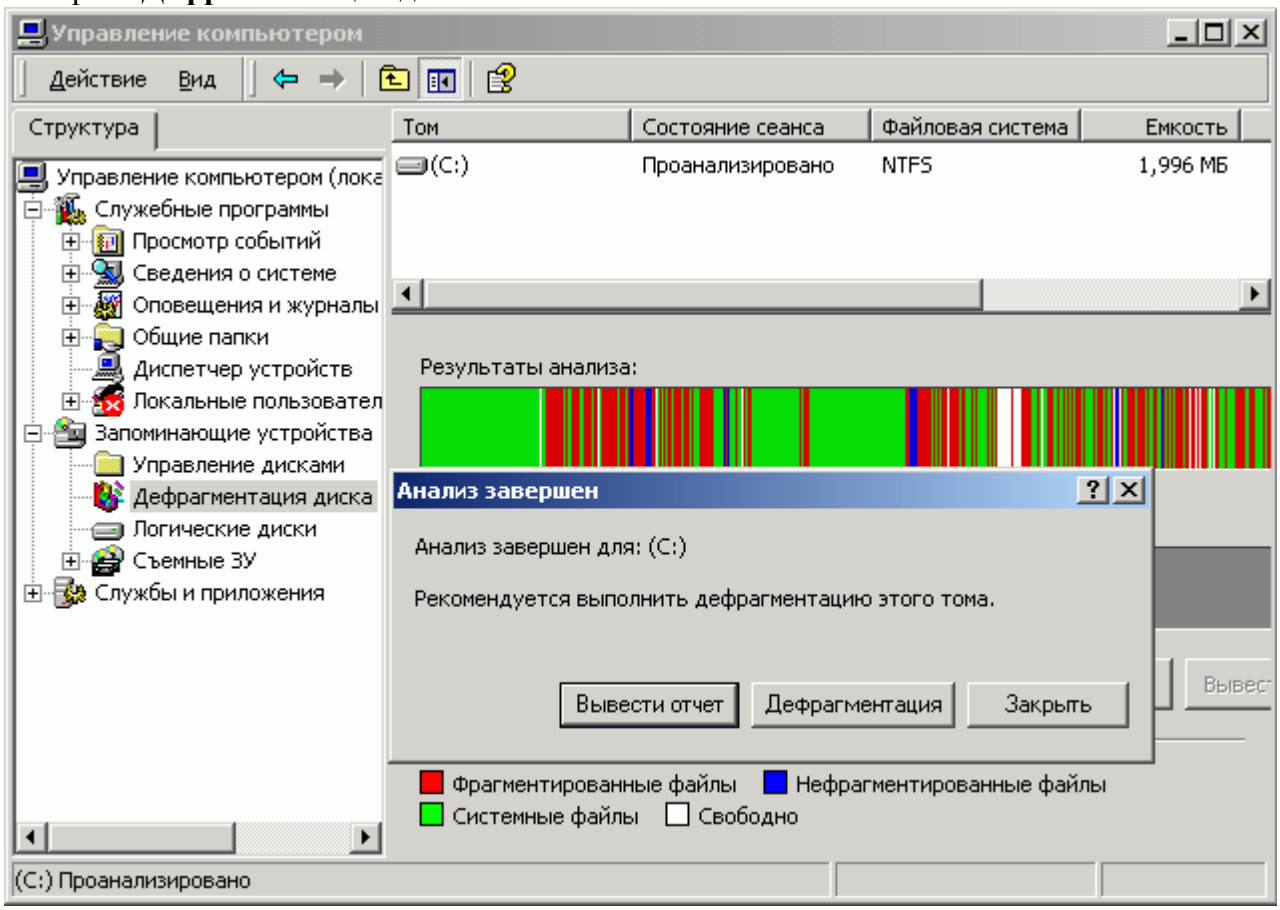
Файловая система на дисках становится фрагментированной после большого количества операций удаления, копирования и создания новых файлов. Файлы могут занимать не одну сплошную последовательную область (экстент), а несколько экстентов, таким образом после образования большого количества мелких несмежных областей после удаления мелких файлов, система размещает крупные файлы во фрагментированном порядке, который вполне естественен, но замедляет доступ к данным на диске.

Из-за большего числа операций с файлами диски на файловых серверах должны дефрагментироваться чаще, чем на рабочих станциях пользователей.

Дефрагментатор — это системная служебная программа, выполняющая поиск и объединение фрагментированных файлов и папок на локальных томах.



Чтобы запустить инструмент "Дефрагментация диска", нажмите **Пуск**, выберите **Программы**, **Администрирование**, а затем **Управление компьютером**. В окне **Управление компьютером** выберите **Дефрагментация диска**.

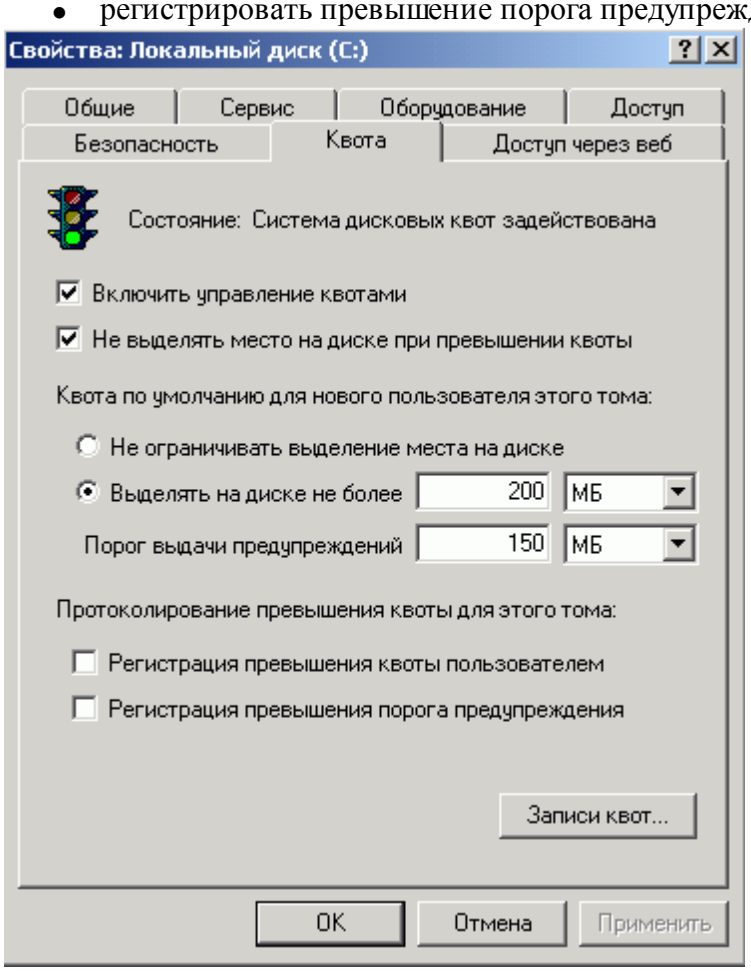


Перед дефрагментацией тома необходимо проанализировать. После проведения анализа выводится диалоговое окно с сообщением о проценте фрагментированных файлов и папок в томе и рекомендацией к действию. Анализ рекомендуется проводить регулярно, а дефрагментацию - только после соответствующей рекомендации программы дефрагментации диска.

Дисковые квоты

Дисковые квоты отслеживают и контролируют использование места на диске для томов. Системные администраторы могут настроить Windows так, чтобы:

- запретить дальнейшее использование места на диске и записать событие в журнал при несоблюдении пользователем ограничения места на диске;
- регистрировать превышение порога предупреждения определенного места на диске.



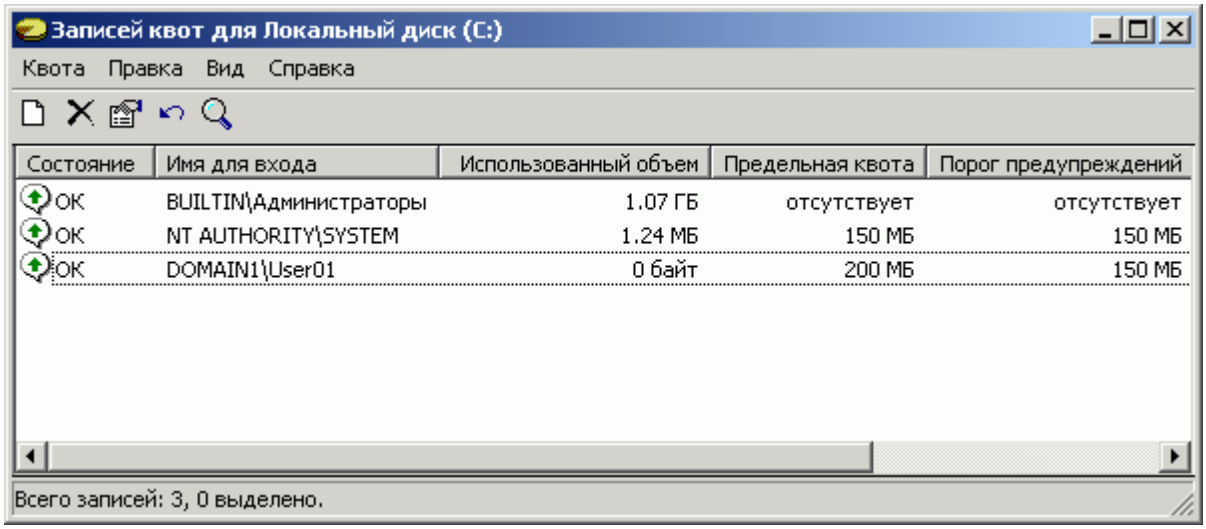
Чтобы настроить дисковые квоты для тома, зайдите в свойства диска и выберите закладку **Квота**.

При включении дисковых квот можно установить два параметра: предельную квоту диска и порог предупреждения дисковой квоты. Предельная квота диска определяет размер места на диске, выделенный данному пользователю. Порог предупреждения дисковой квоты определяет тот уровень, превысив который, пользователь будет находиться около предельной дисковой квоты. Например, можно установить квоту диска для пользователя 200 мегабайт (Мб) и порог предупреждения дисковой квоты 150 Мб. В этом случае пользователь может хранить не более 200 Мб на томе. Если пользователь хранит более 150 Мб на томе, то в системном журнале создается запись о превышении дисковой квоты.

Можно определить, что пользователи могут превышать дисковую квоту. Если нужно проследить использование места на диске каждым пользователем, но при этом не нужно запрещать доступ к тому, необходимо включить дисковую квоту и не ограничивать используемое дисковое место. Можно также настроить регистрацию превышения предельной квоты диска или порога предупреждения дисковой

квоты в журнале.

При включении дисковой квоты для тома новым пользователям автоматически приписывается допустимый размер использования тома. Однако для существующих пользователей тома дисковые квоты не применяются. Чтобы применить квоту к существующему пользователю, нужно создать новую запись в окне записи квот.



Для настройки дисковой квоты с размером, отличным от установленного по умолчанию, необходимо добавить новую запись в список квот. Для этого в свойствах диска на закладке **Квота** нажмите **Записи квот...**.

Для закрепления навыков по использованию средств управления жесткими дисками выполните упражнение Г.

Упражнение 2.Г: "Обслуживание жестких дисков"

Краткое описание

В этом упражнении Вы научитесь просматривать свойства жестких дисков и выполнять настройку дисковых квот.

Предварительные требования к выполнению упражнения

Выполнение упражнения 2.А

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.А по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. На **Рабочем столе** щелкните **Мой компьютер**, а затем **Локальный диск (C:)**. Просмотрите объем диска и свободного места. Обратите внимание, что метку диска можно изменить.
3. В диалоговом окне **Свойства: Локальный диск (C:)** установите на вкладке **Квота** флажки **Включить управление квотами** и **Не выделять место на диске при превышении квоты**.
4. В группе переключателей **Квота по умолчанию для нового пользователя этого тома** выберите вариант **Выделять на диске не более**.
5. В поле **Выделять на диске не более** введите ***100***, измените единицу измерения на ***МБ***.
6. В поле **Порог выдачи предупреждений** введите ***75***, измените единицу измерения на ***МБ***.
7. Нажмите **Применить**. Появится сообщение, предупреждающее, что в случае включения квот будет произведено повторное сканирование этого тома.
8. Нажмите **OK**, потом **Записи квот**.
9. В меню **Квота** выберите команду **Создать запись квоты**.
10. В столбце **Имя** выберите ***user***, нажмите кнопку **Добавить**, а затем нажмите кнопку **OK**, чтобы закрыть диалоговое окно **Выбор пользователей**. Появится диалоговое окно **Добавление новой квоты**. Удостоверьтесь, что применены заданные ранее для диска С пределы квот.
11. Нажмите **OK**, чтобы закрыть окно **Добавление новой квоты**.
12. Закройте окно **Записей квот для Локальный диск (C:)**.
13. Нажмите **OK**, чтобы закрыть окно **Свойства: Локальный диск (C:)**.

Занятие 7: "Автоматизация задач"

Выполнение повседневных задач можно планировать с помощью инструмента "Назначенные задания", который обеспечивает автоматическое выполнение любого приложения в назначенное время. Используя параметры инструмента "Назначенные задания", можно:

- планировать ежедневное, еженедельное или ежемесячное выполнение задания или назначать выполнение задания на другое время;
- изменять график выполнения задания;
- отменять выполнение запланированного задания до или после его начала;
- выполнять запланированное задание немедленно;
- изменять параметры выполнения запланированного задания; например, можно указать, что выполнение задания должно быть отложено, если компьютер работает от аккумуляторов, или назначать выполнение задания после простоя компьютера в течение определенного времени.

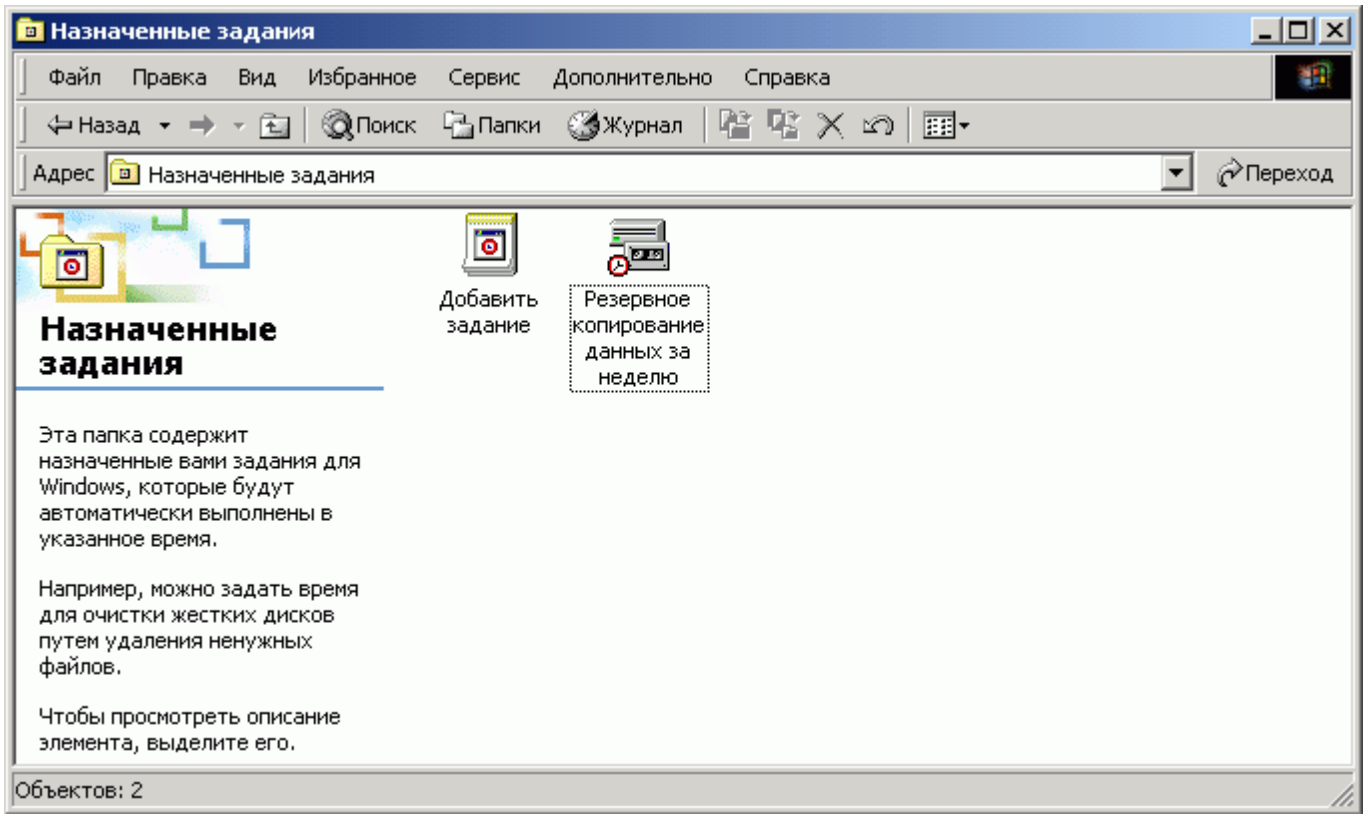
Использование планировщика заданий

Windows 2000 автоматически устанавливает планировщик заданий. Чтобы использовать службу планировщика, дважды щелкните папку **Назначенные задания** на **панели управления**.

Новые задания можно запланировать, дважды щелкнув значок **Добавить задание**, который запускает мастер планирования заданий. Добавлять задания можно путем перетаскивания сценариев, программ или документов из окна проводника Windows или с рабочего стола в окно **Назначенные задания**.

Планировщик заданий позволяет изменять, удалять, выключать или останавливать запланированные задания, просматривать журнал ранее запланированных заданий, а также просматривать задания, запланированные на удаленном компьютере.

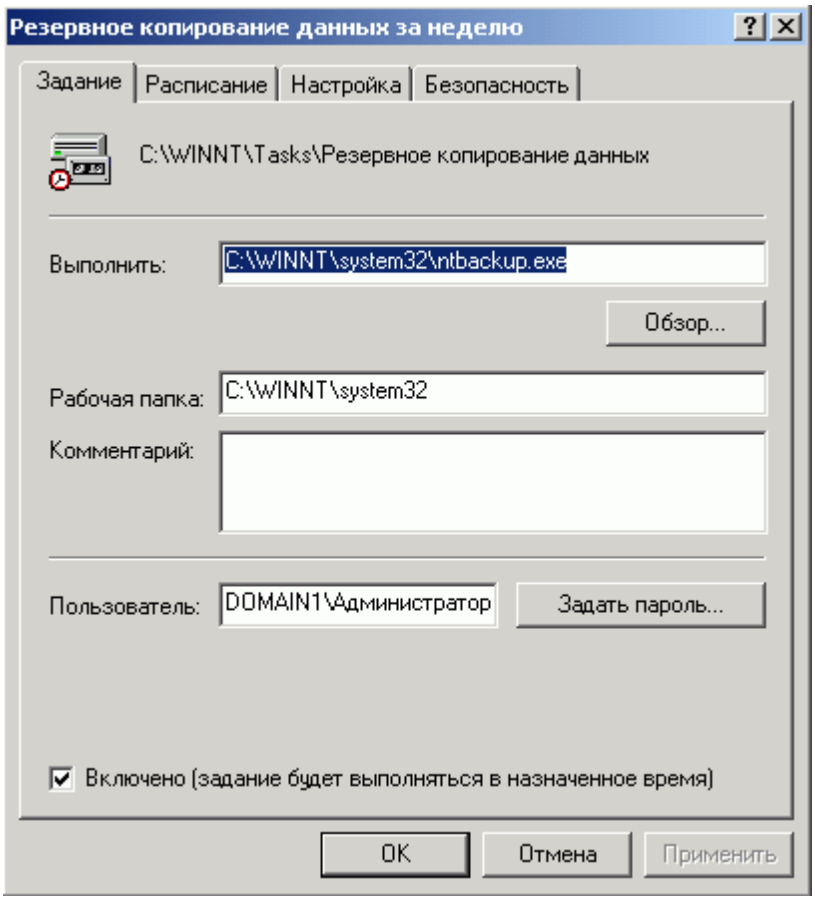
Администраторы сети могут создавать файлы заданий и добавлять их на компьютеры пользователей по мере необходимости. Файлы заданий можно передавать и принимать по электронной почте, а также можно открыть общий доступ к папке **Назначенные задания** и обращаться к ней при помощи папки **Мое сетевое окружение**.



Чтобы выполнить назначенное задание, последовательно выберите **Пуск**, **Программы**, **Стандартные**, **Служебные**, **Назначенные задания**. Щелкните задание правой кнопкой мыши и выберите пункт **Выполнить**.

Устранение неполадок

- В случае невозможности запуска назначенных заданий, убедитесь, что на компьютере запущена служба планировщика заданий.
- Если запланированное задание не выполняется в назначенное время, щелкните правой кнопкой мыши значок задания в списке заданий и выберите **Свойства**. На закладке **Задание** проверьте, что установлен флажок **Включено (задание будет выполняться в заданное время)**. На закладке **Расписание** проверьте, правильно ли задано расписание.



- Если пользователь, учетная запись которого используется для выполнения задания, на момент выполнения еще не вошел в систему, задание выполняется, но не выводится на экран.
- Если программа выполняется неверно, проверьте, указаны ли все необходимые параметры командной строки для данной программы. Чтобы больше узнать о программе и ее параметрах, выполните одно из следующих действий:
  - При наличии справки по программе ознакомьтесь с ней.
  - В командной строке введите следующую команду (где программа представляет имя программы, которую следует запустить): программа /?
  - Проверьте столбец **Состояние** в окне **Назначенные задания**. Следующая таблица содержит типы состояний заданий.

Состояние	**Описание**		
Пусто	Задание не выполняется, либо успешно выполнено	Выполняется	Задание выполняется
Пропущено	Одна или несколько попыток выполнить задание были пропущены		
Запуск не удался	Последняя попытка запуска задачи не удалась		

- Для получения дополнительных сведений о состоянии назначенного задания, в окне выберите пункт меню **Дополнительно**, а затем **Просмотр журнала**

Для закрепления навыков по использованию планировщика задач и выполнению резервного копирования, выполните упражнение Д.

Упражнение 2.Д: "Автоматизация резервного копирования"

Краткое описание

В этом упражнении Вы настроите выполнение процедуры резервного копирования состояния системы локального компьютера по расписанию.

Предварительные требования к выполнению упражнения

Выполнение упражнения 2.А

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.А по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. Последовательно выберите **Пуск**, **Программы**, **Стандартные**, **Служебные**, **Архивация данных**.
3. На закладке **Добро пожаловать!** нажмите кнопку слева от пункта **Мастер архивации**.
4. На странице **Мастер архивации и восстановления Windows 2000** нажмите **Далее**.
5. На странице **Что следует архивировать** установите переключатель **Архивировать только данные состояния системы** и нажмите **Далее**.
6. На странице **Где хранить архив** введите ***C:\Backup.bkf*** и нажмите **Далее**.
7. На странице **Завершение работы мастера архивации** нажмите **Дополнительно**.
8. На странице **Тип архива** убедитесь, что выбран тип **Обычный**, и нажмите **Далее**.
9. На странице **Способы архивации** установите флажок **Проверять данные после архивации** и нажмите **Далее**.
10. На странице **Параметры носителей** нажмите **Далее**, чтобы использовать предлагаемые по умолчанию параметры.
11. На странице **Метка архива** нажмите **Далее**, чтобы использовать предлагаемые по умолчанию параметры.
12. На странице **Когда архивировать** выберите пункт **Позже**
13. Введите в окне **Указание учетной записи** имя пользователя: ***admin***, пароль и подтверждение пароля: ***adminpassword***. Нажмите **ОК**.
14. В строке **Имя задания** введите ***Еженедельное резервное копирование*** и нажмите **Установить расписание...**.
15. На странице **Запланированное задание** в выпадающем списке **Назначить задание** выберите ***Еженедельно***, и поставьте только один флажок напротив текущего дня недели. Установите **время начала** выполнения задания на 5 минут позже по сравнению с текущим моментом.
16. Нажмите **ОК**, чтобы закрыть окно **Запланированное задание**, затем нажмите **Далее**.
17. На странице **Завершение работы мастера архивации** нажмите **Готово**.
18. Когда архивация завершится, нажмите **Закрыть**, чтобы закрыть окно **Ход архивации**, затем

закройте окно **Архивация**.

19. Последовательно выберите **Пуск**, **Настройка**, **Панель управления**, **Назначенные задания**
20. Щелкните правой кнопкой на задание **Еженедельное резервное копирование**, выберите **Свойства**. На закладке **Расписание** проверьте, что установленные параметры соответствуют заданным в пункте 15.
21. Нажмите **ОК**, чтобы закрыть окно **Еженедельное резервное копирование** и щелкните один раз на задание, чтобы в левой части окна **Назначенные задания** появилась информация о его состоянии.
22. Дождитесь запуска задания. По его завершении последовательно выберите пункты **Дополнительно**, **Просмотр журнала**. Пролистайте журнал до конца и посмотрите информацию о выполнении задания.

Тема 3

Протокол TCP/IP: основы адресации

В этой теме:

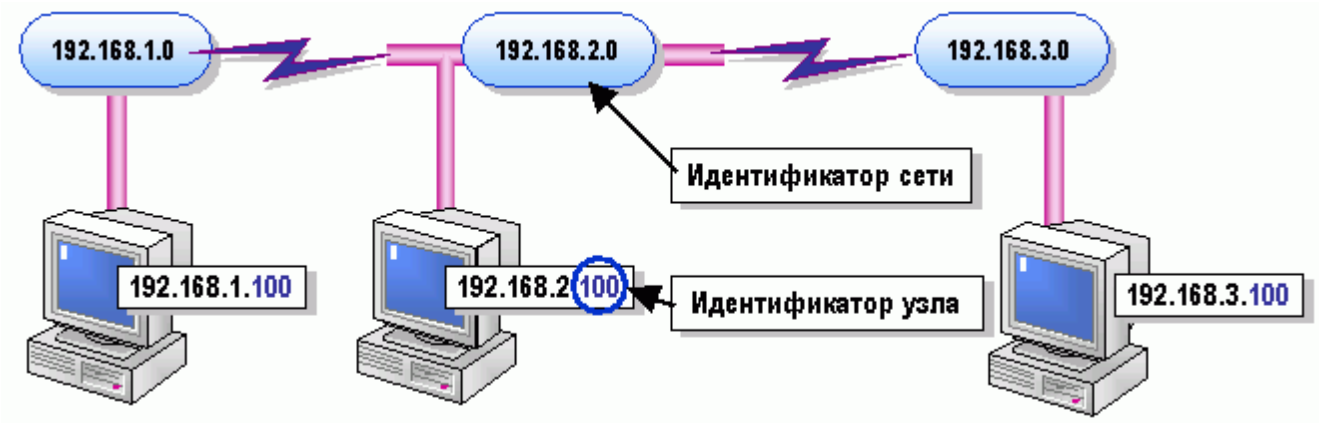
Рассматриваются компоненты IP-адреса и основные термины. Рассказывается о планировании IP-адресации в сети для классового и бесклассового метода адресации. Обсуждаются способы назначения IP-адресов в Windows 2000. Рассматриваются основные проблемы, возникающие при настройке IP-адресов и даются варианты их решения.

Занятие 1: "Компоненты IP-адреса"

IP-адрес - это уникальный идентификатор, который позволяет различать компьютеры в сети, а также определять их местонахождение. Он необходим для каждого компьютера и сетевого устройства (например, маршрутизатор), осуществляющего связь по протоколу TCP/IP.

IP-адрес определяет местоположение компьютера в сети, как почтовый адрес - место дома в городе. Адрес конкретного дома должен отличаться от всех остальных адресов и в то же время соответствовать определенным правилам адресации. Точно так же и IP-адрес, являясь уникальным, должен соответствовать стандартному формату. IP-адрес представляет собой набор из четырех чисел, каждое из которых находится в диапазоне от 0 до 255.

Как адрес дома состоит из двух частей (имени улицы и номера дома), так и IP-адрес содержит два компонента - идентификатор узла и идентификатор сети.



Идентификатор сети

Первой частью IP-адреса является идентификатор сети, определяющий сегмент, в котором находится компьютер. Все компьютеры одного сегмента должны иметь одинаковый идентификатор сети - как дома, находящиеся на одной улице, имеют одинаковое название улицы в почтовом адресе.

Идентификатор узла

Второй частью IP-адреса является идентификатор узла, определяющий компьютер, маршрутизатор или другое устройство в пределах сегмента сети. В пределах одного идентификатора сети каждый идентификатор узла должен быть уникальным - как все дома на одной улице должны иметь разные номера.

Важно отметить, что как два дома на разных улицах могут иметь одинаковые номера домов, два компьютера с разными идентификаторами сети могут иметь одинаковые идентификаторы узла. Однако комбинация идентификатора сети и идентификатора узла для каждого из компьютеров, взаимодействующих друг с другом, должна быть уникальной.

Однозначных правил назначения идентификаторов узла в подсети не существует. Принято нумеровать все узлы TCP/IP последовательно, договорившись о диапазонах используемых адресов.

Шлюз по умолчанию

Один из маршрутизаторов, находящийся в том же сегменте, что и узел, является шлюзом по умолчанию для этого узла. Вся информация, которую узел пересылает в другие сегменты, проходит через шлюз по умолчанию.

Поскольку узел и шлюз по умолчанию находятся в одном сегменте, они имеют одинаковые идентификаторы сети, но разные идентификаторы узла. Например, если узлу присвоен IP-адрес 192.168.2.11, шлюз по умолчанию может иметь IP-адрес 192.168.2.1.

Ограничения при назначении IP-адресов

При назначении IP-адресов необходимо учитывать следующие правила:

- Первый октет (или байт) в идентификаторе сети не может быть равен 127. Идентификатор с этим номером зарезервирован для тестовых подключений, например, локальной петли (local loopback).
- Идентификатор узла не может содержать только "1" во всех битах (или числа 255 для классовой адресации), поскольку соответствующий адрес используется как широковещательный IP-адрес.
- Идентификатор узла не может содержать только "0" во всех битах (или числа 0 для классовой адресации), поскольку соответствующий адрес используется для обозначения идентификатора сети.
- Идентификатор узла должен быть уникален в пределах идентификатора локальной сети.

Занятие 2: "Классовый метод адресации"

Классовый метод IP-адресации предполагает использование трех классов адресов, назначаемых устройствам в IP-сетях. Назначемый класс определяется размером и типом сети. Например, организации, имеющей 200 узлов, назначается сетевой идентификатор класса C, а организации, имеющей 20000 узлов, - идентификатор класса B.

Классы адресов используются для назначения сетевых идентификаторов организациям, что делает возможным подключение их компьютеров к Интернету. Кроме того, классы адресов используются для выделения идентификаторов сети и идентификаторов узла.

Класс A

Адреса класса A присваиваются сетям с очень большим числом узлов. Этот класс допускает наличие 126 сетей, поскольку в качестве идентификатора сети используется первый октет. Остальные три октета образуют идентификатор узла, что обеспечивает поддержку 16 777 214 узлов на сеть.

Класс B

Адреса класса B присваиваются средним и крупным сетям. Этот класс допускает наличие 16 384 сетей, поскольку в качестве идентификатора сети используются первые два октета. Остальные два октета образуют идентификатор узла, что обеспечивает поддержку 65 534 узлов на сеть.

Класс C

Адреса класса C используются для небольших, локальных сетей. Этот класс допускает наличие примерно 2 097 152 сетей, поскольку в качестве идентификатора сети используются первые три октета. Оставшийся октет используется как идентификатор узла, что обеспечивает поддержку 254 узлов на сеть.

Классы D и E

Классы D и E не назначаются узлам. Адреса класса D используются для многоадресной рассылки, а адреса класса E зарезервированы на будущее.

Определение класса адреса

Классовый метод IP-адресации определен структурой IP-адреса и позволяет различать идентификаторы сети и идентификаторы узла, используя упорядоченную систему. IP-адрес состоит из четырех числовых сегментов (байт или октетов) и может быть представлен как ***w.x.y.z***, где ***w***, ***x***, ***y*** и ***z*** - числа в диапазоне от 0 до 255. IP-адреса разделяются на пять классов по значению первого октета - ***w*** в числовом представлении. Это иллюстрирует следующая таблица.

Класс IP-адреса	IP-адрес	Идентификатор сети	Диапазон значений первого октета IP-адреса
A	w.x.y.z	w.0.0.0	1 - 126

B	w.x.y.z	w.x.0.0	128 - 191
C	w.x.y.z	w.x.y.0	192 - 223
D	w.x.y.z	Не существует	224 - 239
E	w.x.y.z	Не существует	240 - 255

Обратите внимание, что в классовой адресации идентификатор сети составляет 1, 2 или 3 полных октета. В случае с бесклассовой схемой адресации (Classless Interdomain Routing - CIDR) может выбираться любая длина идентификатора сети, вне зависимости от класса адреса.

Определение идентификатора сети и идентификатора узла

Для IP-адресов класса A идентификатором сети является первый октет в IP-адресе. Для класса B идентификатором сети являются два первых октета, а для класса C - три первых октета IP-адреса. Остальные октеты определяют идентификатор узла.

Как и IP-адрес, идентификатор сети состоит из четырех октетов. Поэтому, если первый октет в IP-адресе(***w***) представляет собой идентификатор сети, то структура этого идентификатора имеет вид ***w.0.0.0***, где три последних числа имеют нулевые значения. При этом структура идентификатора узла будет иметь вид ***x.y.z***. Обратите внимание, что этому идентификатору не предшествует число 0.

Например, IP-адрес ***172.16.53.46*** является адресом класса B, поскольку ***w*** равняется 172, то есть находится в диапазоне между 128 и 191. Следовательно, идентификатором сети будет **172.16.0.0**, а идентификатором узла - ***53.46*** (точка в конце не ставится).

Технология выделения подсетей

С помощью устройств, таких как маршрутизаторы и мосты, можно расширить сеть, добавив к ней сегменты. Кроме того, с помощью физических устройств можно разделить сеть на меньшие сегменты, чтобы повысить эффективность ее работы. Сегменты сети, разделенные маршрутизаторами, называются ***подсетями***. При создании подсетей необходимо разделить идентификатор исходной сети для задания IP-адресов узлам в подсетях.

Разделение идентификатора сети, используемого для связи через Интернет, для создания меньших (в зависимости от числа указанных IP-адресов) подсетей называется выделением подсети. Теперь для определения нового идентификатора каждой подсети необходимо использовать маску подсети, которая указывает, какая часть IP-адреса должна использоваться в качестве нового идентификатора данной подсети. Определить местоположение узла в сети можно, проанализировав идентификатор сети этого узла. Совпадающие идентификаторы сети показывают, что узлы находятся в одной и той же подсети. Если идентификаторы сети различаются, значит, узлы находятся в разных подсетях, а для установления связи между ними требуется маршрутизатор.

В классовом методе число сетей и узлов, доступных для конкретного класса адреса, определено заранее. Таким образом, у организации, которой назначен идентификатор сети, есть постоянный идентификатор сети и определенное число узлов, ограниченное классом IP-адреса. Используя единственный идентификатор сети, организация может иметь только одну сеть с назначенным числом узлов. Если число узлов велико, одна сеть не сможет обеспечит высокий уровень производительности.

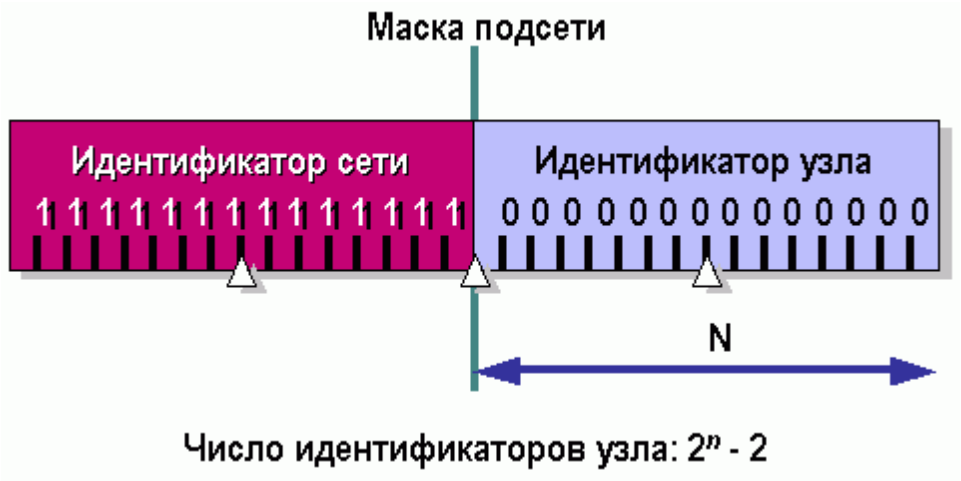
Для решения этой проблемы была разработана технология выделения подсетей. Эта технология позволяет разбить один классовый идентификатор сети для создания меньших (в зависимости от числа указанных IP-адресов) подсетей. При помощи нескольких идентификаторов сети, полученных в

результате этой операции, единая сеть может быть сегментирована на подсети, каждая со своим идентификатором сети, который также называется идентификатором подсети.

Структура масок подсети

Для определения идентификатора сети используется маска подсети. ***Маска подсети*** - это шаблон, который позволяет отличить идентификатор сети от идентификатора узла в IP-адресе. Маска подсети не ограничена правилами, применяемыми в поклассовом методе. Как и IP-адрес, маска подсети представляет собой набор из четырех октетов. Эти числа должны находиться в диапазоне от ***0*** до ***255***.

В классовом методе каждый из этих четырех октетов может принимать только максимальное значение 255 или минимальное значение 0. При этом за максимальными значениями должны следовать минимальные. Максимальные значения представляют идентификатор сети, а минимальные - идентификатор узла. Например, 255.255.0.0 является допустимой маской подсети, а 255.0.255.0 - нет. Маска подсети 255.255.0.0 определяет идентификатор сети как первые два октета IP-адреса.



Маски подсети по умолчанию

В классовом методе каждым класс адреса имеет маску подсети по умолчанию. В следующей таблице приведены маски подсети по умолчанию для каждого адресного класса.

Класс IP-адреса	IP-адрес	Маска подсети	Идентификатор сети	Идентификатор узла
A	w.x.y.z	255.0.0.0	w.0.0.0	x.y.z
B	w.x.y.z	255.255.0.0	w.x.0.0	y.z
C	w.x.y.z	255.255.255.0	w.x.y.0	z

Закрепите полученные навыки по определению класса адресов, выполнив упражнение A.

Специальные маски подсети

При определении существующего идентификатора сети для создания дополнительных подсетей можно использовать любую из приведенных выше масок подсети с любым IP-адресом или идентификатором сети. Поэтому IP-адрес 172.16.2.200 может иметь маску подсети 255.255.255.0 и идентификатор сети 172.16.2.0, а не обязательно маску подсети 255.255.0.0 с идентификатором сети 172.16.0.0, используемую по умолчанию. Это позволяет организации разбивать существующую сеть класса B с идентификатором 172.16.0.0 на меньшие подсети, соответствующие конфигурации их сети.

Определив идентификатор сети узла, легко узнать, является ли другой узел по отношению к нему

локальным или удаленным. Для этого надо просто сравнить идентификаторы сети обоих узлов. Если идентификаторы сети совпадают, то оба узла находятся в одной подсети. Если идентификаторы сети не совпадают, то узлы находятся в разных подсетях, и для обмена данными между ними требуется маршрутизатор.

Пример 1

Рассмотрим два компьютера, А и Б, с IP-адресами 192.168.1.100 и 192.168.2.100 и маской подсети 255.255.0.0. Как показано в приведенной ниже таблице, идентификаторы сети этих IP-адресов совпадают. Следовательно, компьютеры А и Б находятся в одной подсети.

	Компьютер А	**Компьютер Б**
IP-адрес	192.168.1.100	192.168.2.100
Маска подсети	255.255.0.0	255.255.0.0
Идентификатор сети	**192.168.0.0**	**192.168.0.0**

Пример 2

В качестве другого примера рассмотрим компьютеры А и Г с IP-адресами 192.168.1.100 и 192.168.2.100 и маской подсети 255.255.255.0. Как видно из приведенной ниже таблицы, идентификаторы сети этих двух IP-адресов не совпадают. Следовательно, компьютеры А и Г находятся в разных подсетях.

	Компьютер А	**Компьютер Г**
IP-адрес	192.168.1.100	192.168.2.100
Маска подсети	255.255.255.0	255.255.255.0
Идентификатор сети	**192.168.1.0**	**192.168.2.0**

Закрепите полученные навыки по определению локальных и удаленных узлов, выполнив упражнение Б.

Упражнение 3.A: "Определение класса адресов и масок подсетей"

Краткое описание

В этом упражнении Вы получите навыки по определению класса адресов и масок подсетей по умолчанию для заданных IP-адресов.

Порядок выполнения упражнения

В качестве примера определим класс, маску подсети, идентификатор сети и идентификатор узла для IP-адреса **129.102.197.23**

1. По первому октету в IP-адресе определим класс по умолчанию и связанную с ним маску подсети: класс **B**, маска подсети **255.255.0.0**
2. Определим идентификатор сети, взяв числовые значения в IP-адресе, соответствующие по расположению значениям **255** в маске подсети, и заполнив остальную часть адреса нулями: **129.102.0.0**
3. Определим идентификатор узла, взяв числовые значения в IP-адресе, соответствующие по расположению значениям **0** в маске подсети: **197.23**

Повторите эти действия для каждого IP-адреса из приведенной таблицы. Запишите получившиеся результаты (можно распечатать упражнение и записывать прямо в таблицу).

IP-адрес	Класс IP-адреса	Маска подсети	Идентификатор сети	Идентификатор узла
129.102.197.23	B	255.255.0.0	129.102.0.0	197.23
131.107.2.1				
199.32.123.54				
32.12.54.23				
221.22.64.7				
93.44.127.235				
23.46.92.184				
152.79.234.12				
192.168.2.200				
224.224.224.224				
200.100.50.25				
172.71.243.2				

Занятие 3: "Бесклассовый метод адресации"

Разработчики Интернета не предвидели популярности, которую он приобрел сегодня. Они назначали IP-адреса, не задумываясь о проблеме их доступности в будущем. По мере разрастания Интернета количество доступных адресов стало быстро уменьшаться.

Нехватка доступных IP-адресов была вызвана использованием классов для организации IP-сетей. Система классовой IP-адресации оказалась неэффективной, потому что в ней учитываются только три фиксированных размера сетей в Интернете - по одному на каждый из адресных классов: A, B и C. Появление этих классов стало результатом вполне естественного деления значения IP-адреса в десятичной системе.

Исчерпание свободных идентификаторов сетей привело к созданию модернизированной системы адресации, называемой ***методом бесклассовой междоменной маршрутизации*** (***CIDR*** - Classless Inter-Domain Routing). В этой среде IP-адреса и маски подсети представляются в двоичном виде, что позволяет гибко менять традиционные фиксированные размеры сети. Назначение IP-адресов с помощью метода CIDR является более эффективным, чем использование для этой цели классового метода.

Особенности бесклассовой адресации

В методе CIDR все IP-адреса и маски подсети преобразуются в двоичное представление. IP-адреса представляются 32-х разрядными двоичными числами вместо четырех десятичных значений, используемых в системе поклассовой адресации. При таком делении появляется большее количество сетей разных размеров и оптимизируется размещение IP-адресов. Число неиспользуемых адресов невелико, поскольку теперь организации получают минимально необходимое им количество IP-адресов.

В методе CIDR нет предопределенной маски подсети по умолчанию. Вместо этого каждый узел устанавливается с настраиваемой маской подсети, и каждый маршрутизатор пересылает IP-адрес как часть пакета данных. Затем для определения идентификатора сети компьютера, которому предназначается этот пакет, маршрутизатор использует маску подсети, находящуюся в таблице маршрутизации.

Итак, в двоичной системе IP-адрес представлен в виде строки, состоящей из 32 цифр. Эта строка разделяется на четыре поля, называемых октетами или байтами. Каждый октет состоит из восьми бит. Бит имеет значение либо 0, либо 1. Из вышесказанного следует, что 32-битный IP-адрес состоит из 4 байтов.

Последовательность цифр 11011001 представляет собой пример октета в двоичной системе счисления, а последовательность 00001010 11011001 01111011 00000111 является примером представления IP-адреса в двоичной системе. В десятичной системе этот октет и IP-адрес соответственно выражаются числом 217 и значением 10.217.123.7.

Десятичная система счисления

В десятичной системе счисления число представляется следующим образом: сначала следует умножить каждую цифру числа, начиная с крайней справа, на 10 в степени, равной разряду, к которому принадлежит данная цифра (первым из этих множителей является 10°). Сумма полученных чисел и

есть искомое число. Например, число 217 представляется следующим образом:

```
7*100 = 7*1   =   7

1*101 = 1*10  =  10

2*102 = 2*100 = 200

200+10+7 = 217
```

Двоичная система счисления

Для вычисления десятичного значения числа, заданного в двоичном представлении, используется та же методика, что и выше. В этом случае основание 10 заменяется на 2. Затем каждая цифра представления умножается на 2 в степени, равной разряду, к которому принадлежит данная цифра (первым из этих множителей является 20). Например, возьмем то же число 217 в двоичном виде - 11011001 и, начиная с крайней правой цифры, представим его следующим образом:

```
1*20 = 1*1   =   1

0*21 = 0*2   =   0

0*22 = 0*4   =   0

1*23 = 1*8   =   8

1*24 = 1*16  =  16

0*25 = 0*32  =   0

1*26 = 1*64  =  64

1*27 = 1*128 = 128

128+64+0+16+8+0+0+1 = 217
```

Однако, умножать каждую цифру двоичного представления числа на 2 в соответствующей степени для получения эквивалентного десятичного значения утомительно. Этот процесс можно упростить, воспользовавшись программой **Калькулятор** в режиме "Инженерный".

Сравнение двоичного формата масок подсети с десятичным

Маски подсети всегда составлены из ряда последовательно расположенных максимальных значений, за которым следует ряд последовательно расположенных минимальных значений. В двоичном представлении в этом случае за рядом последовательно расположенных единиц идет ряд

последовательных нулей. Ряд последовательно расположенных единиц определяет идентификатор сети, а ряд последовательно расположенных нулей - идентификатор узла. Поскольку маска подсети в двоичном представлении состоит из последовательности единиц, за которыми располагаются нули, каждый ее октет может отображать только некоторое ограниченное количество десятичных значений, как показано в приведенной ниже таблице.

Двоичное представление	Десятичное представление
11111111	255
11111110	254
11111100	252
11111000	248
11110000	240
1110000	224
1100000	192
1000000	128
0000000	0

Закрепите полученные навыки по переводу двоичных значений в десятичные, выполнив упражнение B.

Запись IP-адреса в системе обозначений метода CIDR (префиксная запись)

В системе обозначений метода CIDR используется десятичное представление с точками и битовой маской. Битовая маска задает число последовательно расположенных единиц в двоичном представлении маски подсети, связанной с IP-адресом. Последовательно расположенные друг за другом единицы составляют левые биты маски подсети.

Например, значение IP-адреса в системе обозначений метода CIDR 10.217.123.7/20 указывает на то, что в его маске подсети имеется 20 последовательно расположенных единиц. Следовательно, 12 оставшихся из исходных 32 бит должны быть нулями.

В системе обозначений метода CIDR в конце IP-адреса записывает значение числа бит, определяющих идентификатор сети. Это значение представляется в виде **/x**. Например, 10-битный идентификатор сети отображается как **/10**.

Чтобы вычислить идентификатор сети в том случае, когда IP-адрес указан в системе обозначений метода CIDR:

1. Преобразуйте IP-адрес в двоичное представление.
2. Воспользуйтесь битовой маской для определения числа бит в IP-адресе, составляющих идентификатор сети.
3. Добавьте в идентификатор сети недостающие нули для получения четырехоктетной структуры.

Если IP-адрес и маска подсети заданы в десятичном представлении, необходимо преобразовать маску подсети в двоичное представление и выполнить ту же процедуру.

Пример

Рассмотрим IP-адрес 10.217.123.7/20. Поскольку в его маску подсети входит 20 последовательно расположенных единиц, первые двадцать бит идентификатора сети составлены из бит IP-адреса, за которыми следуют нули. В представленной ниже таблице видно, как вычисляется идентификатор сети

в двоичном формате.

IP-адрес	00001010 11011001 01111011 00000111
Маска подсети	11111111 11111111 11110000 00000000
Идентификатор сети	00001010 11011001 01110000 00000000

После вычисления идентификатора сети в двоичном формате, следует преобразовать его в десятичное представление с точками для того, чтобы с ним могли работать пользователи.

Определение локального и удаленного узла назначения

После того, как определен идентификатор сети, компьютер путем сравнения собственного идентификатора сети с аналогичным параметром узла назначения устанавливает, является этот узел локальным или удаленным. В результате становится понятным, требуется ли посылать пакет на маршрутизатор или его надо посылать напрямую в локальную подсеть.

Пример локального узла

Рассмотрим два IP-адреса 10.217.123.7/10 и 10.218.102.31/10, принадлежащие соответственно компьютеру A и компьютеру B. В приведенных ниже таблицах представлены результаты вычисления двух идентификаторов сети, по которым определяется, являются ли узлы локальными или удаленными по отношению друг к другу.

	Компьютер A	**Компьютер B**
IP-адрес	**00001010 11**011001 01111011 00000111	**00001010 11**011010 01100110 00000011
Маска подсети	**11111111 11**000000 00000000 00000000	**11111111 11**000000 00000000 00000000
Идентификатор сети (двоичное представление)	**00001010 11**000000 00000000 00000000	**00001010 11**000000 00000000 00000000
Идентификатор сети (десятичное представление)	**10.192**.0.0	**10.192**.0.0

Как видно из приведенных таблиц, идентификаторы сети двух IP-адресов совпадают. Следовательно, компьютеры A и B находятся в одной подсети.

Пример удаленного узла

В качестве другого примера рассмотрим два IP-адреса 10.217.123.7/20 и 10.218.102.31/20, принадлежащие компьютеру A и компьютеру E. В приведенных ниже таблицах представлены результаты вычисления двух идентификаторов сети, по которым определяется, являются ли узлы локальными или удаленными по отношению друг к другу.

	Компьютер A	**Компьютер E**
IP-адрес	**00001010 11011001 0111**1011 00000111	**00001010 11011010 0110**0110 00000011
Маска подсети	**11111111 11111111 1111**0000 00000000	**11111111 11111111 1111**0000 00000000
Идентификатор сети (двоичное представление)	**00001010 11011001 0111**0000 00000000	**00001010 11011010 0110**0000 00000000

Идентификатор сети (десятичное представление)	**10.217.112**.0	**10.218.96**.0

Как видно из приведенных таблиц, идентификаторы сети двух IP-адресов не совпадают. Следовательно, компьютеры A и E находятся в разных подсетях.

Объединение подсетей

Чтобы избежать несоответствующего назначения адресов, в методе CIDR используется объединение подсетей. Стратегия объединения подсетей состоит в объединении нескольких адресов среды с поклассовой адресацией в единый идентификатор сети среды с бесклассовой маршрутизацией. Благодаря данной методике, несколько идентификаторов сети класса C объединяются в один идентификатор CIDR сети. В системе обозначений метода CIDR идентификатор сети представляется в виде числа бит маски подсети аналогично тому, как выглядит IP-адрес. Например: 192.168.0.0/22.

Деление сети на подсети

При использовании методики объединения подсетей каждой организации назначается один идентификатор сети службы CIDR, представляющий единую сеть. Однако при работе с большой единой сетью ее эффективность снижается из-за увеличения нагрузки на сеть и увеличения задержек при пересылке пакетов.

Организация может физически разделить свою сеть на подсети при помощи маршрутизаторов. Поскольку каждая подсеть нуждается в собственном идентификаторе, единый идентификатор CIDR сети, полученный для всей организации, следует разделить на идентификаторы подсетей меньшего размера. Процесс разделения идентификатора подсети на идентификаторы меньших подсетей называется ***делением сети на подсети***. Идентификаторы сетей меньшего размера называются также ***идентификаторами подсетей***.

В рассмотренном выше примере получившая единый идентификатор сети организация имеет возможность разделить свою сеть на сегменты меньшего размера. Такая операция проводится с использованием подходящей маски подсети. После физического разделения сети важно провести ее логическое деление на подсети, создаваемые для каждого ее сегмента.

После этого организация назначает идентификатор каждой из подсетей, исходя из количества имеющихся в них компьютеров. Однако из-за того, что разделение сети является внутренним процессом, любой маршрутизатор, находящийся вне сети организации, не может видеть выделенные в ней подсети и их идентификаторы.

Например, если организации потребуется не более 62 компьютеров в каждой подсети, можно воспользоваться маской подсети 255.255.255.192.

Упражнение 3.Б: "Определение локального и удаленного узла назначения"

Краткое описание

В этом упражнении Вы научитесь отличать узлы, находящиеся в одной подсети, от узлов, находящихся в разных подсетях, по IP-адресу и маске подсети.

Порядок выполнения упражнения

Используйте маски подсети, чтобы отделить идентификаторы сети от идентификатора узла и сравните идентификаторы сети обоих узлов. Если они совпадают, то оба узла находятся в одной подсети, если не совпадают, то узлы находятся в разных подсетях.

Повторите эти действия для каждой пары компьютеров. Запишите получившиеся результаты (можно распечатать упражнение и записывать прямо в таблицу).

Пример:

	Компьютер А	**Компьютер Б**
IP-адрес	192.168.1.100	192.168.2.100
Маска подсети	255.255.255.0	255.255.255.0
Идентификатор сети	192.168.1.0	192.168.2.0

Вывод: компьютеры находятся в разных подсетях.

Задание 1

	Компьютер А	**Компьютер Б**
IP-адрес	172.18.35.110	172.19.35.111
Маска подсети	255.255.255.0	255.255.255.0
Идентификатор сети		

Вывод:

Задание 2

	Компьютер А	**Компьютер Б**
IP-адрес	17.18.35.110	17.19.35.111
Маска подсети	255.0.0.0	255.0.0.0
Идентификатор сети		

Вывод:

Задание 3

	Компьютер А	**Компьютер Б**
IP-адрес	9.9.9.9	9.10.11.12
Маска подсети	255.255.0.0	255.255.0.0
Идентификатор сети		

Вывод:

Задание 4

	Компьютер А	**Компьютер Б**
IP-адрес	206.51.69.17	206.51.96.18
Маска подсети	255.255.255.0	255.255.255.0
Идентификатор сети		

Вывод:

Задание 5

	Компьютер А	**Компьютер Б**
IP-адрес	126.17.12.17	126.71.21.71
Маска подсети	255.0.0.0	255.0.0.0
Идентификатор сети		

Вывод:

Упражнение 3.B: "Преобразование десятичных чисел в двоичные и обратно"

Краткое описание

В этом упражнении Вы получите навыки по преобразованию десятичных чисел в двоичные и двоичных чисел в десятичные.

Порядок выполнения упражнения

Преобразование чисел из одной системы счета в другую можно делать вручную или с помощью инструмента **Калькулятор** в режиме **Инженерный**. Например, преобразуем значение IP-адреса **131.107.2.200** в двоичное представление в следующем порядке:

1. Запустим **Калькулятор** в режиме **Инженерный**.
2. По очереди преобразуем четыре числа из десятичного в двоичное значения, добавив недостающие до октета нули.
3. В двоичном представлении IP-адрес **131.107.2.200** будет выглядеть как **10000011.01101011.00000010.11001000**

Повторите эти действия для каждого IP-адреса из приведенной таблицы. Запишите получившиеся результаты (можно распечатать упражнение и записывать прямо в таблицу) и переходите ко второму заданию.

IP-адрес в десятичном представлении	IP-адрес в двоичном представлении
122.131.25.64	01111010.10000011.00011001.01000000
215.34.211.9	
97.49.153.122	
64.144.25.100	
176.34.68.78	
42.89.215.61	
71.73.65.166	
47.245.235.84	
156.213.67.23	
124.87.235.87	
7.23.87.2	

Во втором задании Вам необходимо перевести IP-адреса из двоичного представления в десятичное. Запишите получившиеся результаты.

IP-адрес в двоичном представлении	IP-адрес в десятичном представлении
01110110.00011010.10101111.01011101	118.26.175.93
10101001.01010101.10101010.11011000	
00011011.11011000.10110101.01010111	

01111111.11100000.00000101.00101011	
11000100.10101100.01100001.11101111	
01110111.00111100.10111000.10101001	
10100011.11101101.10100010.10101110	
01010101.01100100.11110111.10101000	
00111100.00111010.10101000.10101111	
01010111.10111100.11101110.10101010	

Занятие 4: "Назначение IP-адресов в Windows 2000"

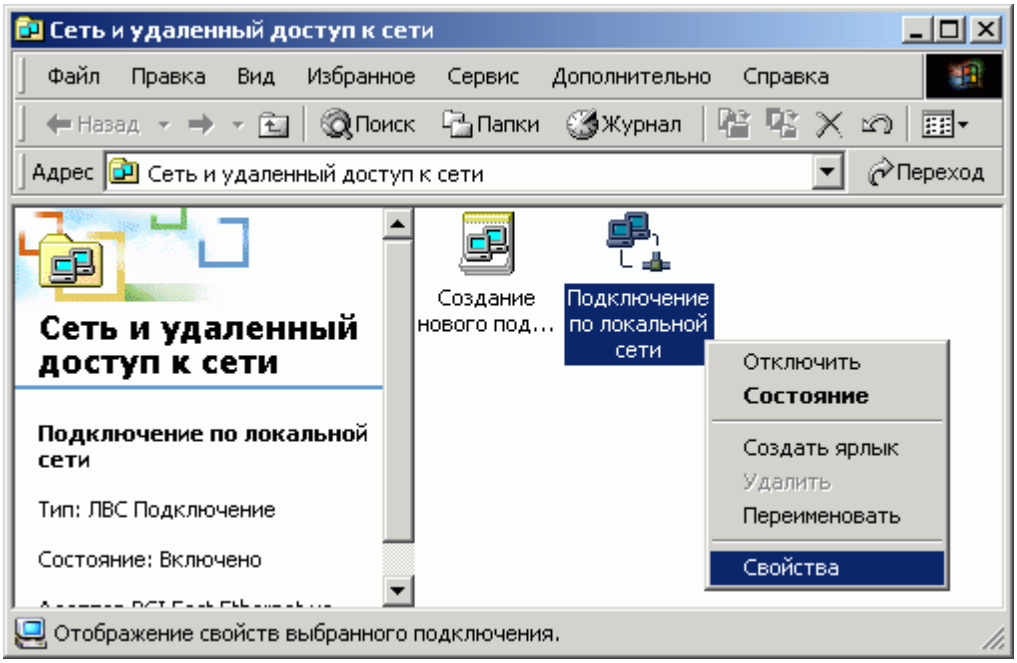
Существует два метода назначения IP-адресов - статический и автоматический. При использовании статического метода адрес каждого компьютера в сети необходимо настроить вручную. Автоматический метод позволяет централизованно настроить IP-адреса для всей сети, а затем динамически назначить их каждому компьютеру.

Назначив IP-адрес, можно посмотреть его с помощью диалогового окна **Свойства**: **Протокол Интернета (TCP/IP)** или с помощью инструмента **Ipconfig**.

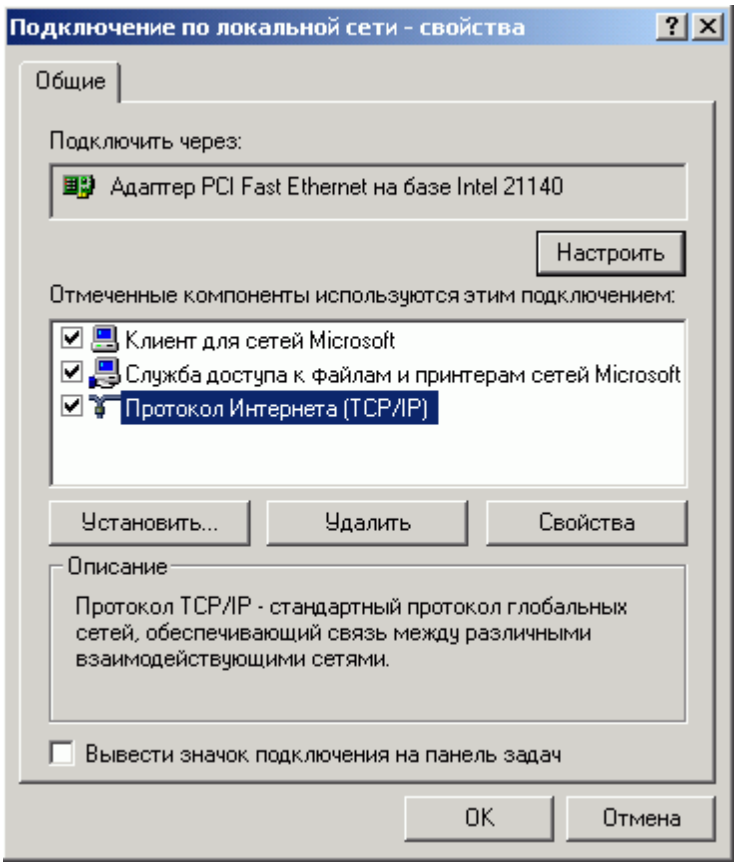
Статическая IP-адресация

Статическая IP-адресация подразумевает настройку IP-адресов вручную. Диалоговое окно **Свойства**: **Протокол Интернета (TCP/IP)** в операционной системе Windows 2000 позволяет вручную назначить IP-адрес узлу или устройству TCP/IP. Чтобы открыть диалоговое окно свойств TCP/IP, выполните следующие действия:

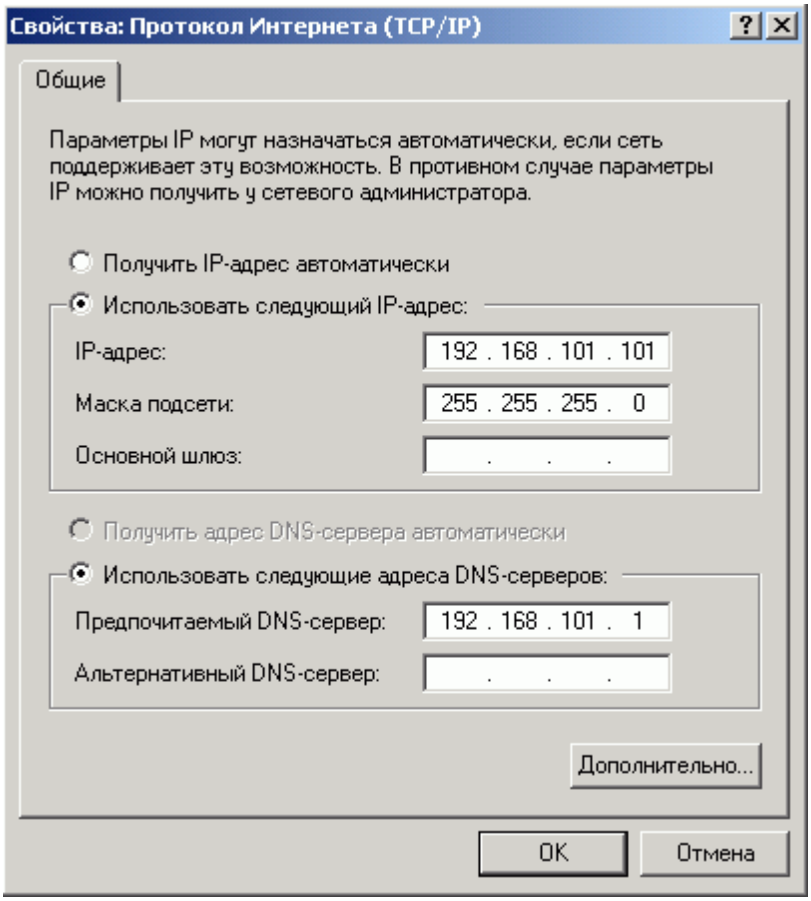
1. В меню **Пуск** укажите команду **Настройки** и выберите **Сеть и удаленный доступ к сети**.
2. В окне **Сеть и удаленный доступ к сети** правой кнопкой мыши щелкните значок **Подключение по локальной сети** и выберите команду **Свойства**.



3. В диалоговом окне **Подключение по локальной сети - свойства** выделите элемент **Протокол Интернета (TCP/IP)**, затем выберите **Свойства** для вывода диалогового окна **Свойства**: **Протокол Интернета (TCP/IP)**.



4. В этом диалоговом окне выберите **Использовать следующий IP-адрес** для ввода IP-адреса, маски подсети и адреса шлюза по умолчанию.

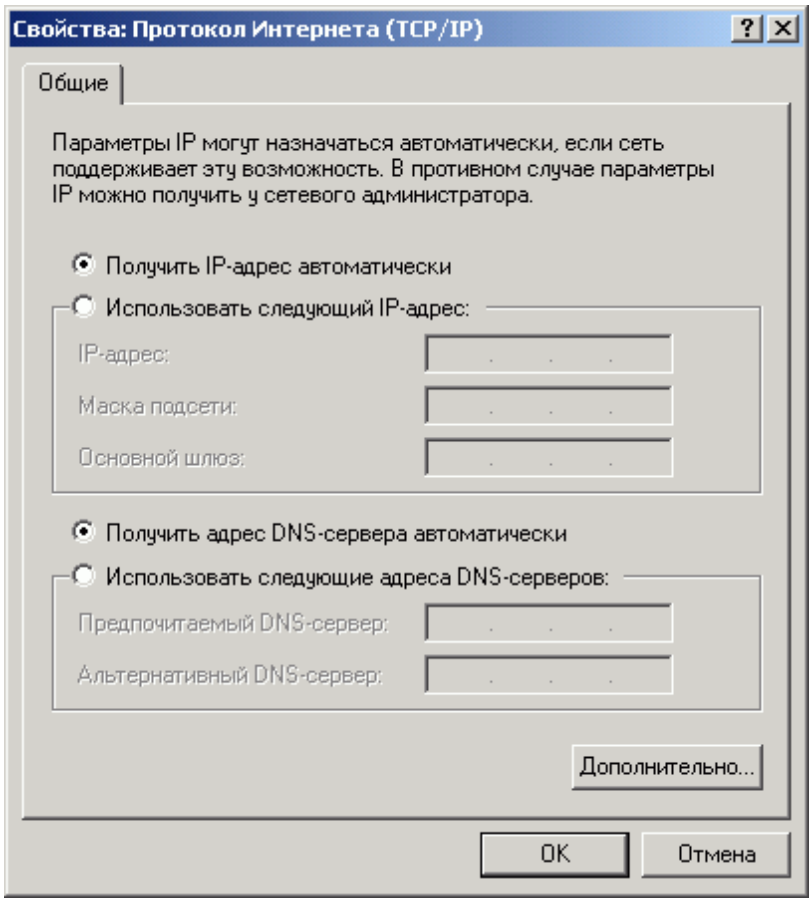


Как правило, компьютер имеет одну сетевую плату, и поэтому для него нужен только один IP-адрес. Если в каком-либо устройстве, например в маршрутизаторе, установлено несколько сетевых плат, каждая плата должна иметь собственный IP-адрес.

DHCP (Dynamic Host Configuration Protocol)

Протокол DHCP является стандартом TCP/IP для упрощения настройки и назначения IP-адресов в объединенной сети. Протокол DHCP использует сервер DHCP для управления процессом динамического распределения IP-адресов. Серверы DHCP содержат базу данных с IP-адресами, которые можно назначать узлам сети.

Для автоматического получения адресов с помощью DHCP узлы сети должны быть настроены на использование этого протокола. Чтобы активизировать DHCP, выберите **Получить IP-адрес автоматически**. Операционная система Windows 2000 использует этот вариант по умолчанию.



Использование протокола DHCP уменьшает объем административной работы, связанной с перенастройкой компьютеров в сетях TCP/IP, а также снижает ее сложность. При перемещении компьютера из одной подсети в другую необходимо изменить его IP-адрес, указав новый идентификатор сети. Протокол DHCP позволяет автоматически назначить узлу (называемому также клиентом DHCP) IP-адрес из базы данных, содержащей адреса, назначенные подсети. Кроме того, если компьютер временно отключается от сети, сервер DHCP может назначить его адрес другому узлу.

Автоматическое назначение личных IP-адресов (Automatic Private IP Addressing - APIPA)

Если сервер DHCP недоступен и IP-адрес не может быть назначен автоматически, операционная система Windows 2000 выбирает адрес в зарезервированном корпорацией Microsoft классе IP-адресации, имеющем диапазон от 169.254.0.1 до 169.254.255.254. Этот адрес используется, пока не будет обнаружен сервер DHCP. Такой метод получения IP-адреса называется автоматической IP-адресацией (Automatic Private IP Addressing - APIPA). С его помощью нельзя назначить IP-адрес шлюза по умолчанию или адрес сервера DNS, поскольку он предназначен только для небольших сетей,

состоящих из одного сегмента.

Определение метода назначения IP-адреса

Иногда требуется узнать IP-адрес конкретного компьютера. Например, если компьютер не может наладить связь с другими компьютерами в сети или другие компьютеры не могут связаться с ним. В этом случае для выяснения причины неполадки необходимо узнать IP-адреса других компьютеров.

Информацию о статической настройке TCP/IP можно просмотреть с помощью диалогового окна **Свойства: Протокол Интернета (TCP/IP)** или инструмента **ipconfig**.

Диалоговое окно "Свойства: Протокол Интернета (TCP/IP)"

С помощью диалогового окна **Свойства: Протокол Интернета (TCP/IP)** можно определить, выполнялась ли настройка IP-адреса динамически или статически. Тем не менее, если IP-адрес был настроен динамически с помощью DHCP или автоматически операционной системой Windows 2000, определить значения параметров конфигурации TCP/IP невозможно. Параметры конфигурации включают IP-адрес, маску подсети и основной шлюз. Определить эти значения можно только в том случае, если была выполнена статическая настройка.

Ipconfig

Операционная система Windows 2000 позволяет просматривать информацию о настройках TCP/IP с помощью служебной программы Ipconfig, работающей в режиме командной строки. Чтобы получить подробную информацию с помощью программы **Ipconfig**, задайте ключ **all**. Для этого введите **ipconfig /all** в командной строке.

На экран будут выведены сведения обо всех параметрах конфигурации TCP/IP. Теперь можно проверить, настроен ли компьютер на использование протокола DHCP. Если значение параметра **DHCP разрешен** равно **Да** и отображен IP-адрес сервера DHCP, значит, IP-адрес был получен с помощью DHCP.

Если в момент назначения IP-адреса сервер DHCP был недоступен и адрес был задан автоматически, перед IP-адресом будет указано слово *автонастройка*. Параметр **Автонастройка включена** в этом случае будет иметь значение **Да**. Кроме того, не будет отображен IP-адрес сервера DHCP.

Более подробно о использовании инструмента **Ipconfig** смотрите занятие 5.

Упражнение 3.Г: "Настройка статического IP-адреса"

Краткое описание

В этом упражнении Вы настроите установленную в упражнении 1.А Windows 2000 Professional на использование статического IP-адреса.

Предварительные требования к выполнению упражнения

Необходимо иметь компьютер с установленной операционной системой Windows 2000 Professional (то есть выполнить упражнение 1.А), на которую Вы имеете права локального администратора.

Порядок выполнения упражнения

Внимание! Эту операцию рекомендуется проводить только на тестовом компьютере, установленным специально для обучения, иначе взаимодействие с другими компьютерами по сети может прекратиться.

1. Войдите в операционную систему под учетной записью пользователя, имеющего права локального администратора. При выполненном упражнении 1.А по установке Windows 2000 Professional используйте учетную запись пользователя ***Администратор*** с паролем ***password***.
2. Откройте список сетевых подключений: **Пуск**, **Настройка**, **Сеть и удаленный доступ к сети**.
3. Правой кнопкой щелкните **Подключение по локальной сети** и выберите **Свойства**.
4. Из перечня компонентов выберите **Протокол Интернета (TCP/IP)** и нажмите **Свойства**.
5. Установите флажок в поле **Использовать следующий IP адрес**, введите в поле **IP адрес** значение **192.168.101.102**, а в поле **Маска подсети** значение **255.255.255.0**.
6. Нажмите **ОК** три раза подряд.
7. Чтобы проверить, что установленный Вами адрес вступил в действие, последовательно выберите: **Пуск**, **Выполнить...** и введите команду **cmd**.
8. В командной строке введите **ipconfig /all**. Убедитесь, что текущие настройки IP-адреса и маски подсети совпадают с теми, что Вы установили. Кроме того, убедитесь, что напротив строчки **DHCP разрешен** написано **Нет**. Это значит, что адрес установлен статически, а не получен автоматически от DHCP сервера, как было настроено ранее.

Занятие 5: "Диагностика проблем при настройке IP-адресов и их решение"

Просмотр конфигурации с помощью команды ipconfig /all

Устраняя неполадки сетевых соединений TCP/IP, начинайте с проверки конфигурации TCP/IP на том компьютере, где возникают эти неполадки. Для получения сведений о настройках сетевых интерфейсов, включая его IP-адрес, маску подсети и основной шлюз, можно использовать программу **ipconfig**.

Когда команда **ipconfig** выполняется с параметром **/all**, она выдает подробный отчет о настройках всех интерфейсов, включая все настроенные последовательные порты. Результаты работы команды **ipconfig /all** можно перенаправить в файл и вставить их в другие документы. Можно также использовать эти результаты для проверки конфигурации TCP/IP на всех компьютерах сети и для выявления причин неполадок TCP/IP-сети.

Например, если компьютер имеет IP-адрес, который уже присвоен другому компьютеру, то маска подсети будет иметь значение 0.0.0.0.

На следующем примере показаны результаты работы команды **ipconfig /all** на компьютере, настроенном на использование DHCP-сервера для автоматической настройки TCP/IP и адреса DNS-сервера для разрешения имен.

```
Настройка протокола IP для Windows 2000

        Тип узла . . . . . . . . . . . . : Гибридный
        Включена IP-маршрутизация . . . . : Нет
        Доверенный WINS-сервер. . . . . . : Нет

Адаптер Ethernet Подключение по локальной сети:

        Имя компьютера  . . . . . . . . . : student1.microinform.ru
        DNS-серверы  . . . . . . . . . . . : 192.168.100.10
        Описание  . . . . . . . . . . . . : 3Com 3C90x Ethernet Adapter
        Физический адрес  . . . . . . . . : 00-60-08-3E-46-07
        DHCP разрешен  . . . . . . . . . . : Да
        Автонастройка включена  . . . . . : Да
        IP-адрес  . . . . . . . . . . . . : 192.168.100.112
        Маска подсети . . . . . . . . . . : 255.255.255.0
        Основной шлюз . . . . . . . . . . : 192.168.100.1
        DHCP-сервер . . . . . . . . . . . : 192.168.100.10
        Основной WINS-сервер  . . . . . . : 192.168.100.10
        Дополнительный WINS-сервер  . . . : 192.168.100.11
        Аренда получена . . . . . . . . . : 2 сентября 2002 г. 18:32:13
        Аренда истекает . . . . . . . . . : 5 сентября 2002 г. 18:32:13
```

Обновление конфигурации с помощью команды ipconfig /renew

Если компьютер настроен на использование DHCP и получает конфигурацию от DHCP-сервера, можно инициировать обновление аренды, выполнив команду **ipconfig /renew**.

Когда выполняется команда **ipconfig /renew**, все сетевые адаптеры компьютера, на котором используется DHCP (за исключением настроенных вручную), пытаются связаться с DHCP-сервером и обновить свои имеющиеся или получить новые конфигурации. Можно также выполнить команду **ipconfig** с параметром **/release**, чтобы немедленно освободить текущую конфигурацию DHCP для узла.

Если с конфигурацией TCP/IP все в порядке, следующим шагом должна быть проверка возможности соединения с другими узлами TCP/IP-сети.

Проверка соединений с помощью программы ping

Команда **ping** позволяет проверить работоспособность IP-соединения. С помощью команды **ping** можно отправить эхо-запрос ICMP интересующему узлу по имени узла или по его IP-адресу. Используйте команду **ping**, чтобы проверить, может ли узел взаимодействовать с другими узлами по протоколу TCP/IP. Команду **ping** можно также использовать для выявления неполадок сетевых устройств и неправильных настроек.

Обычно лучше всего проверять наличие маршрута между локальным компьютером и узлом сети, обращаясь сначала к узлу с помощью команды **ping** и IP-адреса этого узла. Для этого выполните следующую команду:

ping *IP-адрес*

Используя команду **ping**, следует выполнить перечисленные ниже действия.

1. Обратитесь по адресу замыкания на себя, чтобы проверить правильность настройки и установки TCP/IP на локальном компьютере.

   ping 127.0.0.1
2. Обратитесь по IP-адресу локального компьютера, чтобы убедиться в том, что он был правильно добавлен к сети.

   ping *IP-адрес_локального_узла*
3. Обратитесь по IP-адресу шлюза по умолчанию, чтобы проверить его работоспособность и возможность связи с узлами в локальной сети.

   ping *IP-адрес_шлюза_по_умолчанию*
4. Обратитесь по IP-адресу удаленного узла, чтобы проверить возможность связи с узлами через маршрутизатор.

   ping *IP-адрес_удаленного_узла*

Команда **ping** использует разрешение имен компьютеров в IP-адреса в стиле Windows Sockets. Поэтому, если обратиться по адресу удается, а по имени - нет, то проблема связана с разрешением имен или адресов, а само соединение с сетью исправно.

Если обращение с помощью команды **ping** на каком-либо этапе оканчивается неудачей, убедитесь, что:

- после установки и настройки протокола TCP/IP компьютер был перезагружен;
- IP-адрес локального компьютера является допустимым и правильно отображается на вкладке **Общие** диалогового окна **Свойства: Протокол Интернета (TCP/IP)**;
- включена IP-маршрутизация и связь между маршрутизаторами функционирует нормально.

Команда **ping** может выполняться с различными параметрами, задающими такие характеристики, как размер пакетов, число отправляемых пакетов и срок жизни пакета (TTL), и определяющими, нужно ли записывать используемый маршрут и нужно ли устанавливать флаг, запрещающий фрагментацию пакетов. Выполните команду **ping -?** для просмотра возможных параметров.

На следующем примере показано, как можно отправить два пакета размером по 1450 байт по IP-адресу 172.16.48.10:

```
C:\>ping -n 2 -l 1450 172.16.48.10
Обмен пакетами с 172.16.48.10 по 1450 байт:

Ответ от 172.16.48.10: число байт=1450 время
```

По умолчанию команда **ping** ожидает возврата каждого запроса в течение 1000 мс (1 секунда), а потом выдает сообщение "Превышен интервал ожидания для запроса". Если удаленная система, к которой выполняется обращение, использует соединение с большими задержками, например спутниковую связь, то для возврата запроса потребуется большее количество времени. Чтобы увеличить время ожидания, используйте параметр **-w**.

Устранение неполадок имен NetBIOS с помощью программы nbtstat

NetBIOS через TCP/IP (NetBT) разрешает имена NetBIOS в IP-адреса. TCP/IP предоставляет много способов разрешения имен NetBIOS, включая поиск в локальном кэше, запросы к WINS-серверу, широковещательные запросы, запросы к DNS-серверу и поиск в файлах Lmhosts и Hosts.

Программа Nbtstat - это полезное средство для устранения неполадок с разрешением имен NetBIOS. Команду **nbtstat** можно использовать для удаления или исправления предварительно загруженных записей:

- **nbtstat -n** выводит имена, зарегистрированные службами локального компьютера, например службами "Сервер" и "Рабочая станция".
- **nbtstat -c** отображает кэш имен NetBIOS, который содержит сопоставления имен с адресами для других компьютеров.
- **nbtstat -R** очищает кэш имен и перезагружает его из файла Lmhosts.
- **nbtstat -RR** освобождает имена NetBIOS, зарегистрированные на WINS-сервере, а затем обновляет их регистрацию.
- **nbtstat -a** *имя* выполняет запрос о состоянии адаптера NetBIOS к компьютеру, заданному параметром *имя*. Запрос состояния адаптера возвращает локальную таблицу имен NetBIOS этого компьютера и аппаратный адрес его сетевого адаптера.
- **nbtstat -S** перечисляет текущие сеансы NetBIOS и их состояние, а также статистику, как показано в следующем примере. `Таблица подключений NetBIOS`

```
Локальное имя           Состояние        Вид          Удаленный узел       Ввод
Вывод
-------------------------------------------------------------------------------
-------------------
CORP1               Подключен       Исх             CORPSUP1         6MB            5MB
CORP1               Подключен       Исх             CORPPRINT      108KB          116KB
CORP1               Подключен       Исх             CORPSRC1       299KB           19KB
```

```
CORP1                Подключен       Исх             CORPEMAIL1     324KB          19KB
CORP1                Ожидание
```

Трассировка сетевых соединений с помощью программы tracert

Tracert (Trace Route) - это служебная программа для трассировки маршрутов, используемая для определения пути, по которому IP-датаграмма доставляется по месту назначения. Для определения сетевого маршрута от одного узла сети до другого команда **tracert** использует поле срока жизни (TTL) заголовка IP и ICMP-сообщения об ошибках.

Описание работы tracert

Программа Tracert определяет маршрут до конечного узла, посылая конечному узлу эхо-пакеты протокола ICMP (Internet Control Message Protocol) с различными значениями поля срока жизни (TTL) протокола IP. Каждый маршрутизатор, через который проходит путь, обязан перед дальнейшей пересылкой пакета уменьшить значение его поля TTL по меньшей мере на 1. Когда значение поля TTL становится равным нулю, маршрутизатор обязан послать компьютеру-отправителю ICMP-сообщение об истечении времени.

Команда tracert определяет маршрут, посылая первый эхо-пакет с полем TTL, равным 1, и увеличивая значение этого поля на единицу для каждого последующего отправляемого эхо-пакета до тех пор, пока конечный узел не ответит или пока не будет достигнуто максимальное значение поля TTL. Маршрут определяется путем анализа ICMP-сообщений "Time Exceeded", отправленных промежуточными маршрутизаторами. Некоторые маршрутизаторы просто отбрасывают сообщения с истекшим сроком жизни, поэтому они невидимы для служебной программы Tracert.

Команда **tracert** выводит упорядоченный список интерфейсов маршрутизаторов, возвративших ICMP-сообщение об истечении времени. Если используется параметр **-d**, служебная программа Tracert не выполняет поиск имен DNS для IP-адресов.

В следующем примере пакет должен пройти два маршрутизатора (10.0.0.1 и 192.168.0.1), чтобы достигнуть узла 172.16.0.99. Шлюз по умолчанию для узла имеет адрес 10.0.0.1, а IP-адресом маршрутизатора в сети 192.168.0.0 является адрес 192.168.0.1.

```
 C:\>tracert 172.16.0.99 -d
Трассировка маршрута к 172.16.0.99 с максимальным числом прыжков 30:
1     2 мс     3 мс     2 мс  10.0.0.1
2    75 мс    83 мс    88 мс  192.168.0.1
3    73 мс    79 мс    93 мс  172.16.0.99
Трассировка завершена.
```

Устранение неполадок с помощью tracert

Команду **tracert** можно использовать для определения места в сети, в котором нарушается нормальная передача пакетов. В следующем примере основной шлюз определил, что не существует подходящего пути к узлу 192.168.10.99. Причиной может быть неправильная конфигурация маршрутизатора или отсутствие сети с адресом 192.168.10.0 (неправильный IP-адрес).

C:\>tracert 192.168.10.99

Трассировка маршрута к 192.168.10.99 с максимальным числом прыжков 30:

1 10.0.0.1 сообщает: Заданная сеть недоступна.

Трассировка завершена.

Программа Tracert полезна при устранении неполадок в больших сетях, когда к одному и тому же узлу могут вести несколько путей.

Тема 4

Службы DNS и DHCP

В этой теме:

Рассматриваются две основные сетевые службы в Windows 2000: DNS и DHCP. Разбирается, как они должны работать и описывается их реализация в Windows 2000.

Занятие 1: "Автоматическое назначение IP-адресов с помощью службы DHCP"

Основные определения DHCP

Протокол DHCP (Dynamic Host Configuration Protocol) - стандартный протокол стека TCP/IP, упрощающий управление настройками IP-адресов узлов. Задача протокола DHCP - динамическое распределение IP-адресов и дополнительных параметров стека TCP/IP DHCP-клиентам в сети.

Каждый компьютер, работающий в сети на основе протокола TCP/IP, должен иметь уникальные имя и IP-адрес. IP-адрес (вместе с соответствующей маской подсети) определяет и компьютер, и подсеть, к которой он присоединен. Когда компьютер перемещается в другую подсеть, IP-адрес необходимо изменить. Служба DHCP позволяет динамически назначать IP-адрес клиенту из базы данных IP-адресов на DHCP-сервере в локальной подсети.

Принцип работы DHCP

Служба DHCP использует модель «клиент-сервер». Сетевой администратор устанавливает один или несколько DHCP-серверов, которые предоставляют параметры настройки стека протоколов TCP/IP клиентам. База данных сервера содержит следующие параметры:

- Допустимые настройки для всех клиентов в сети.
- Допустимые IP-адреса для назначения клиентам и зарезервированные адреса для ручного назначения.
- Продолжительность аренды, предоставляемой сервером. Аренда определяет промежуток времени, в течение которого арендованный IP-адрес может использоваться.

При установленном и настроенном DHCP-сервере клиенты, поддерживающие DHCP, могут при каждом запуске и входе в сеть динамически получать IP-адреса и дополнительные параметры настройки.

Преимущества использования службы DHCP

При администрировании сетей на базе TCP/IP служба DHCP обеспечивает следующие преимущества:

Безопасная и надежная настройка

Служба DHCP позволяет избежать ошибок настройки, возникающих из-за ручного ввода значений на каждом компьютере. Также DHCP помогает предотвратить конфликты адресов, вызываемые использованием ранее арендованного IP-адреса при настройке нового компьютера в сети.

Проще управлять настройками

Используя DHCP-сервера, можно существенно уменьшить время настройки и перенастройки компьютеров в сети, в том числе благодаря поддержке дополнительных настроек при назначении

аренды адреса. Кроме того, процесс обновления аренды IP-адреса гарантирует, что частое обновление настроек пользователя (например, пользователей с переносными компьютерами, которые часто переезжают с места на место) может быть выполнено автоматически при подключении клиента к сети.

Терминология DHCP

Область — это последовательный диапазон IP-адресов, зарезервированный для автоматического выделения IP-адресов из него. Обычно область - это часть отдельной физической подсети, в которой используется служба DHCP. Области используются сервером для управления распределением и назначением IP-адресов и всех связанных с ними дополнительные параметры стека TCP/IP DHCP-клиентам в сети.

Суперобласть - набор областей, сгруппированных вместе. Она обычно используется для поддержки нескольких логических IP-подсетей в одной физической подсети. Суперобласти содержат только список отдельных областей или дочерних областей, которые могут быть активизированы вместе.

Диапазон исключения — это последовательность IP-адресов в области, исключаемая из области. Диапазоны исключения гарантируют, что никакой адрес из этих диапазонов не будет предлагаться сервером DHCP-клиентам в сети.

Доступный **пул адресов** формируется из адресов, оставшихся после определения области DHCP и диапазонов исключения адреса. Адреса из пула используются сервером для назначения DHCP-клиентам в сети.

Аренда — это интервал времени, задаваемый DHCP-сервером, в течении которого компьютер-клиент может использовать арендованный IP-адрес. После назначения клиенту IP-адреса аренда становится активной. Клиент автоматически обновляет аренду на сервере перед истечением ее срока. Аренда становится недействительной либо после истечения срока действия, либо после удаления на сервере.

Резервирование используется для создания DHCP-сервером постоянной связи адреса с адресом сетевой карты. Резервирование гарантирует, что компьютер с этой сетевой картой всегда будет использовать один и тот же IP-адрес.

Дополнительные параметры стека TCP/IP предоставляют дополнительные возможности по настройке клиентов. DHCP-сервер может назначать эти параметры одновременно с IP-адресом. Наиболее часто используются такие параметры, как IP-адрес шлюза по умолчанию (маршрутизатора) и IP-адрес DNS-сервера.

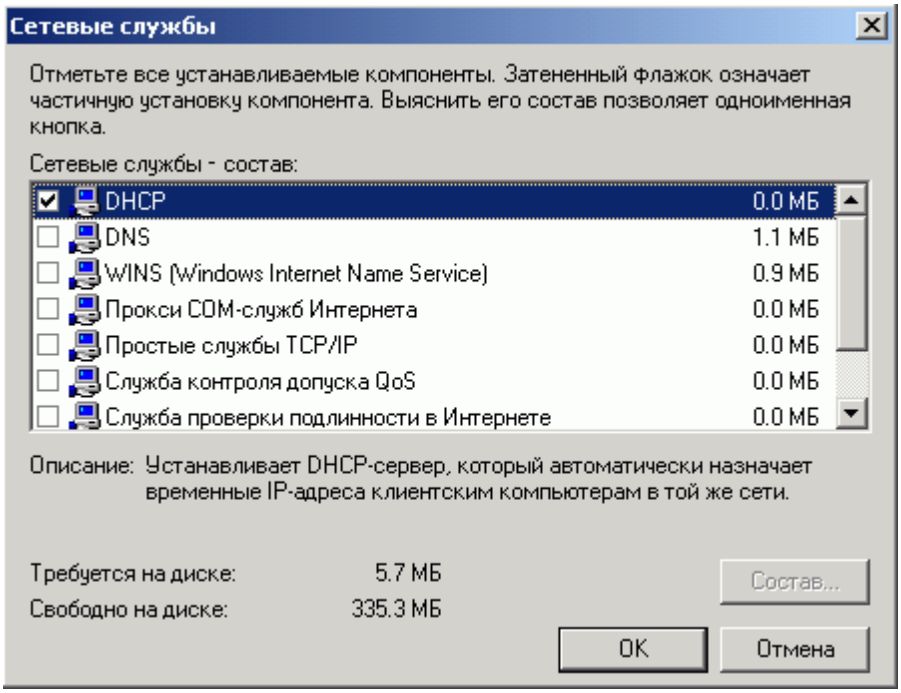
Занятие 2: "Реализация службы DHCP в Windows 2000"

Windows 2000 Server включает в себя службу DHCP, которая используется для автоматизации назначения IP-адресов и прочих параметров протокола TCP/IP в сети.

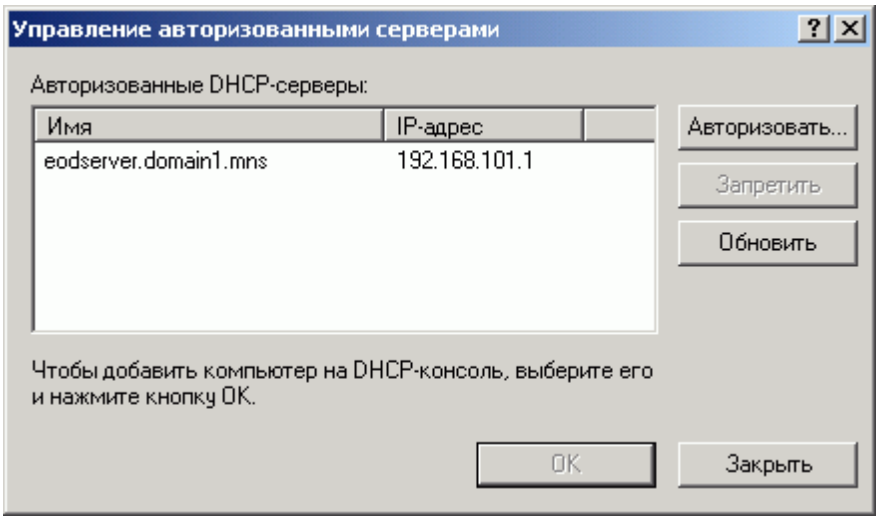
Основное средство для управления службой DHCP - консоль **DHCP**, которая добавляется в папку **Администрирование** на панели управления при установке DHCP-сервера в Windows 2000 Server.

Порядок установки и настройки службы DHCP

1. Определите диапазон или диапазоны IP-адресов, для которых DHCP должен будет предоставлять услуги настройки в сети.
2. Настройте свойства протокола TCP/IP для сервера, на котором работает служба DHCP, на статическую адресацию (более подробно смотрите в занятии 4 темы 3).
3. Установите службу DHCP, добавив ее в **Мастере компонентов Windows**, в списке **Сетевые службы**.

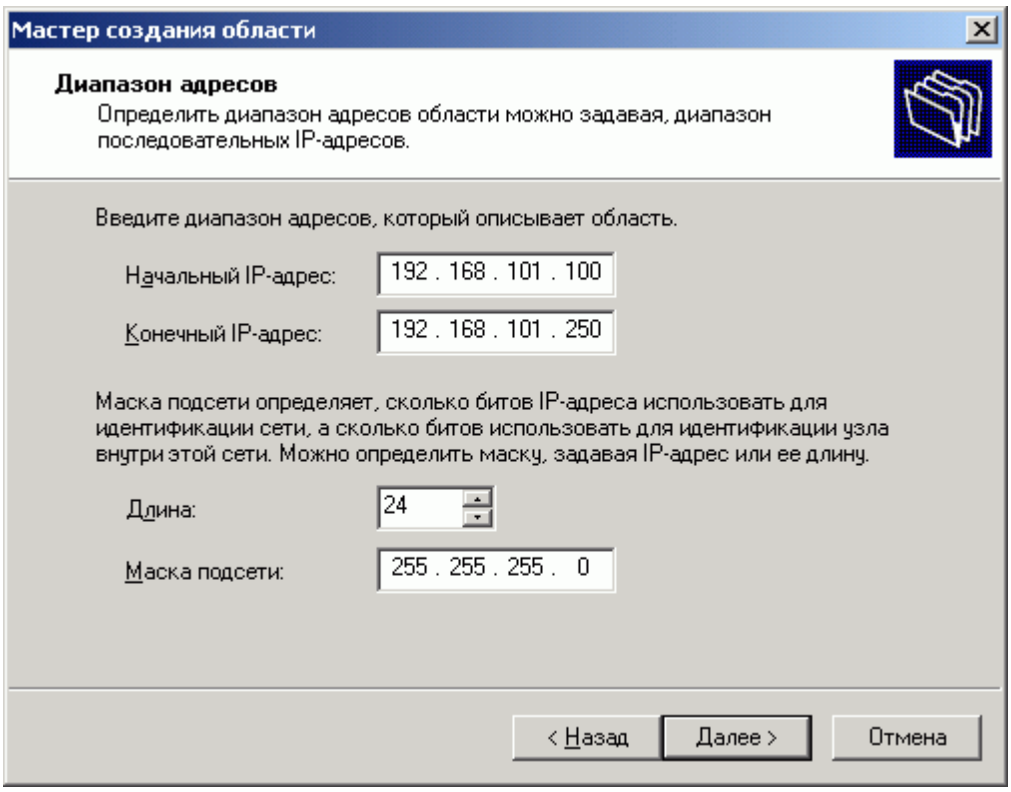


4. Откройте консоль DHCP. Для этого нажмите кнопку **Пуск** и выберите **Программы**, **Администрирование** и **DHCP**.
5. Авторизуйте сервер DHCP в Active Directory (это необходимо, если в сети предприятия есть контроллеры домена Active Directory). В консоли щелкните узел **DHCP**, в меню **Действие** выберите **Список авторизованных серверов**. В окне **Управление авторизованными серверами** нажмите **Авторизовать...** и введите имя или IP-адрес авторизуемого DHCP-сервера. Для выполнения этой операции необходимо войти в систему с учетной записью члена группы "Администраторы предприятия".

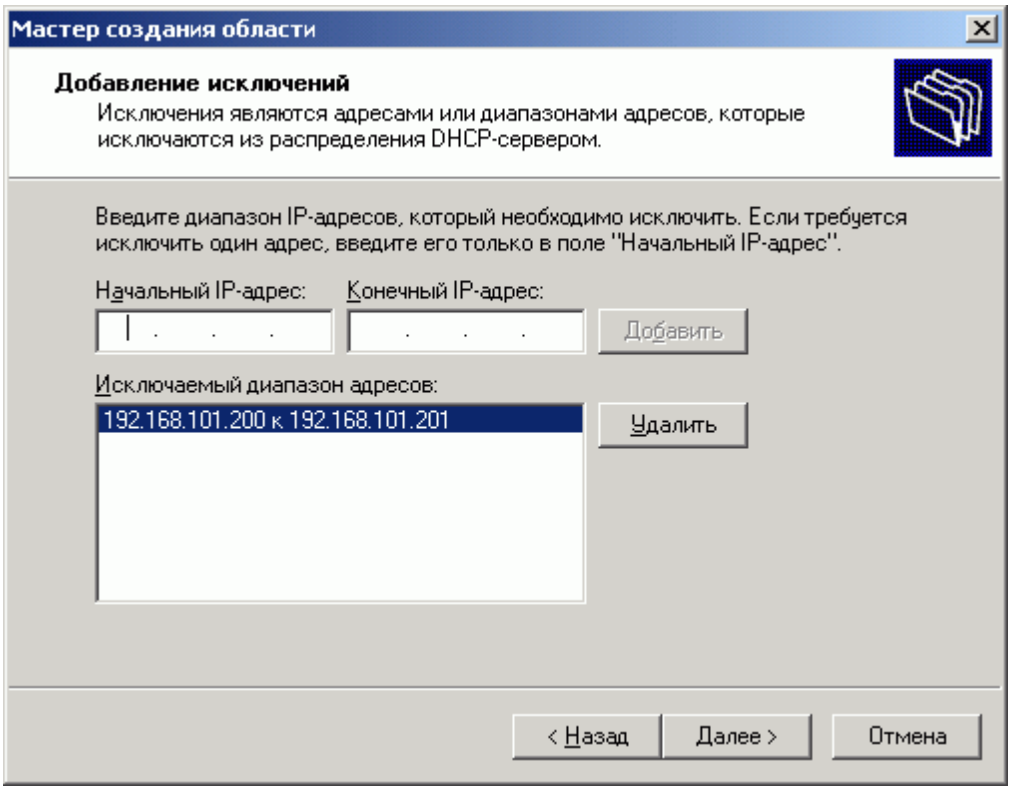


6. Создайте новую область:

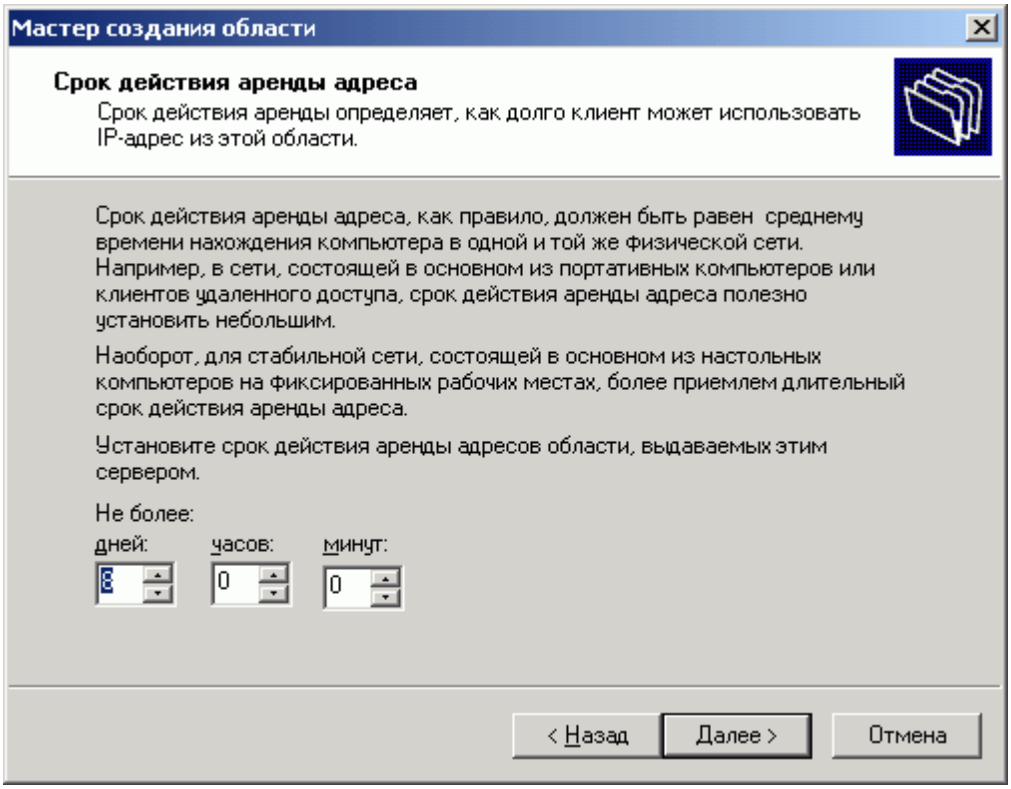
Введите диапазон адресов, которые будут выдаваться клиентам.



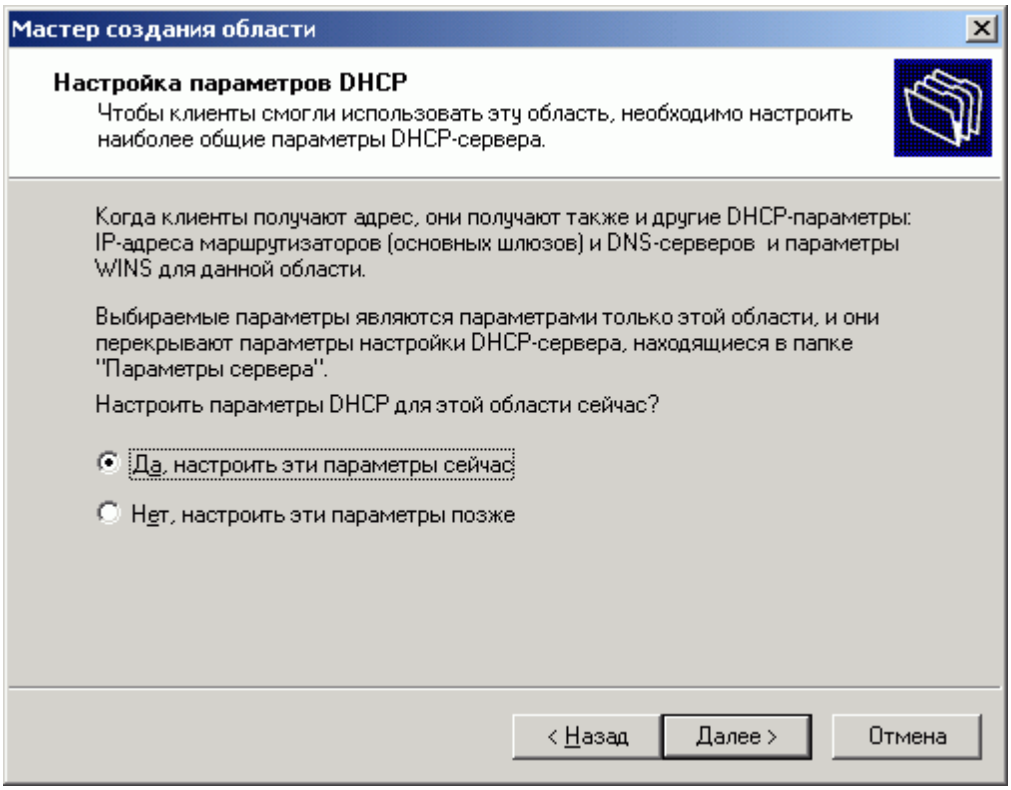
Если необходимо, исключите диапазоны IP-адресов, которые не должны предоставляться сервером в данной области.



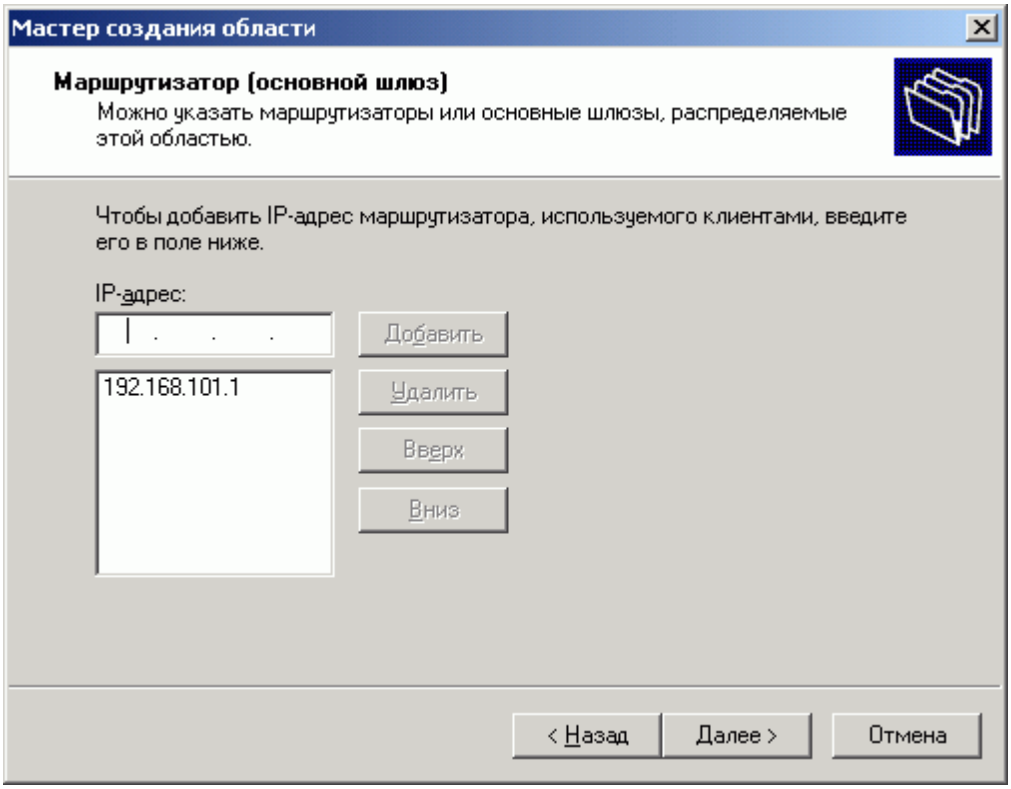
Установите срок, на который адрес должен выдаваться клиентам. 8 дней - вполне приемлемый срок по умолчанию, и в большинстве случаев не стоит изменять этот параметр.



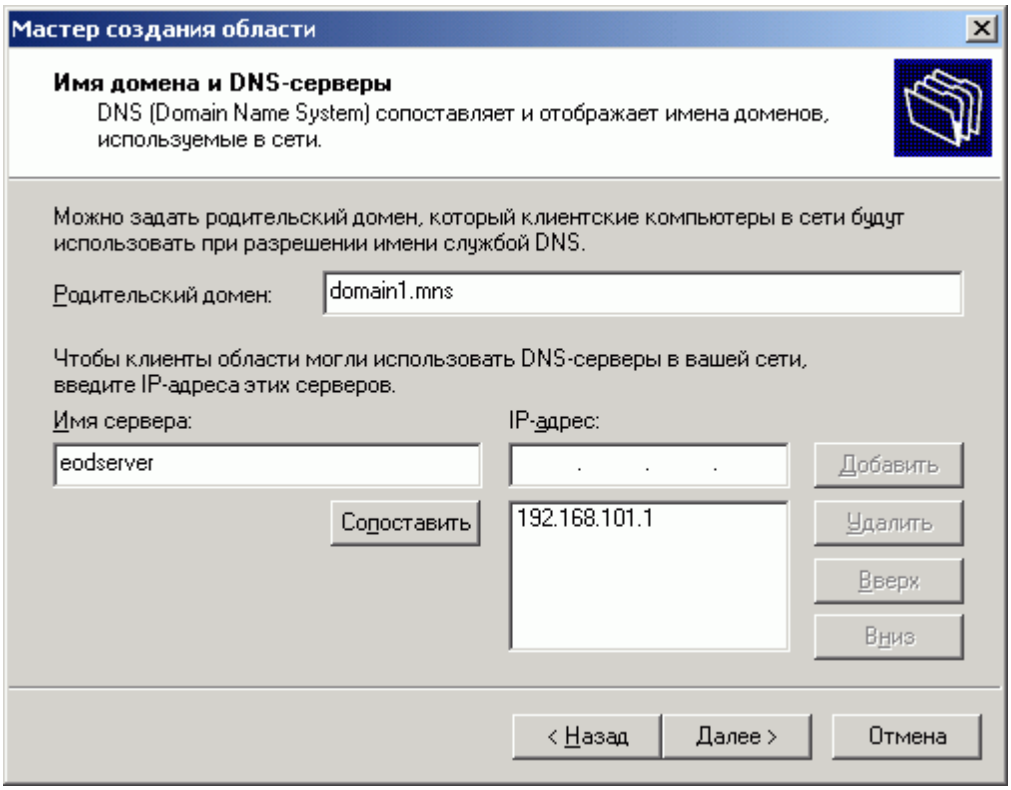
Кроме IP-адреса, клиент может получать дополнительные параметры. Рекомендуется настраивать эти параметры при создании области. Для Windows 2000 клиентов ключевыми являются адрес шлюза по умолчанию (маршрутизатора) и адрес DNS сервера.



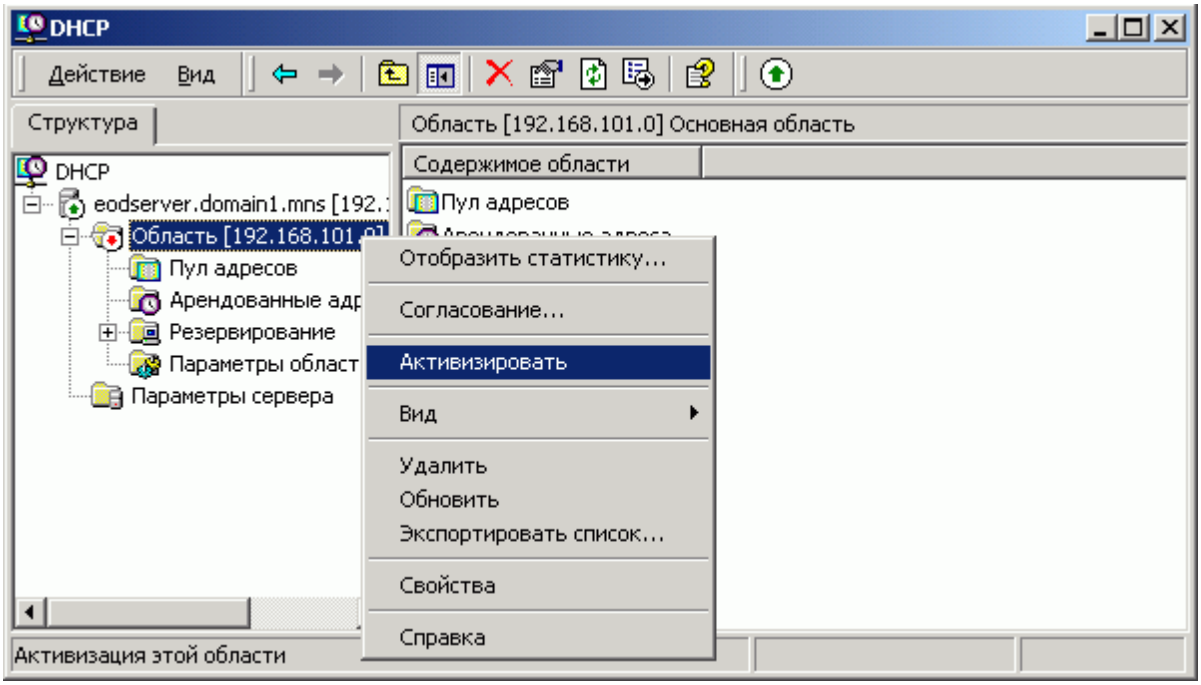
Если адрес маршрутизатора не будет указан, клиент не сможет посылать пакеты за пределы подсети. Более подробно о протоколе TCP/IP см. тему 3.



Для входа в домен Active Directory клиенты используют DNS сервер для поиска контроллера домена. Если адрес DNS сервера не указан, у клиентов будут проблемы со входом в домен. Более подробно о интеграции Active Directory и DNS см. занятие 3 темы 5.



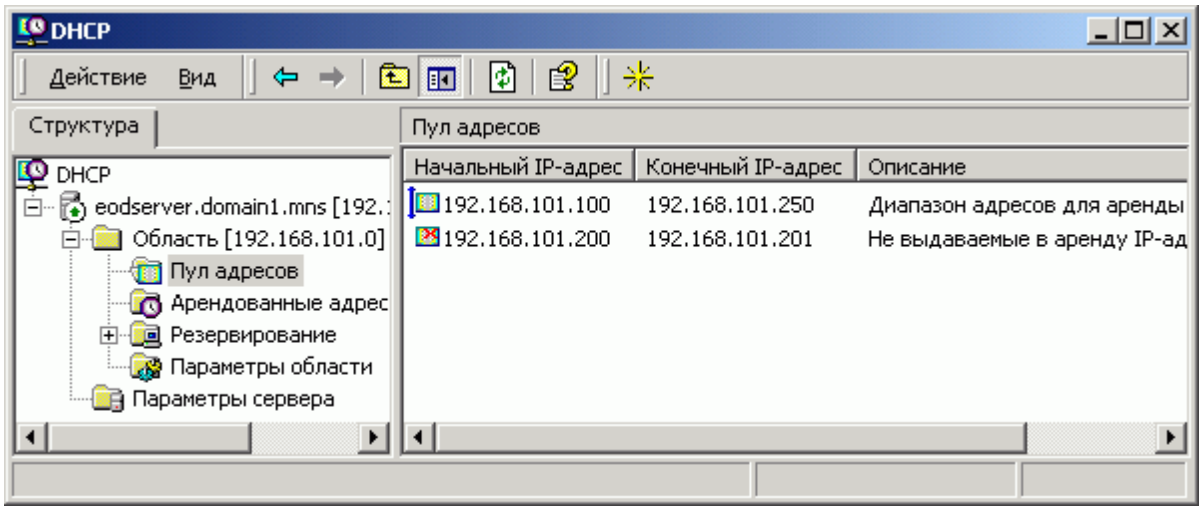
7. Активизируйте область.



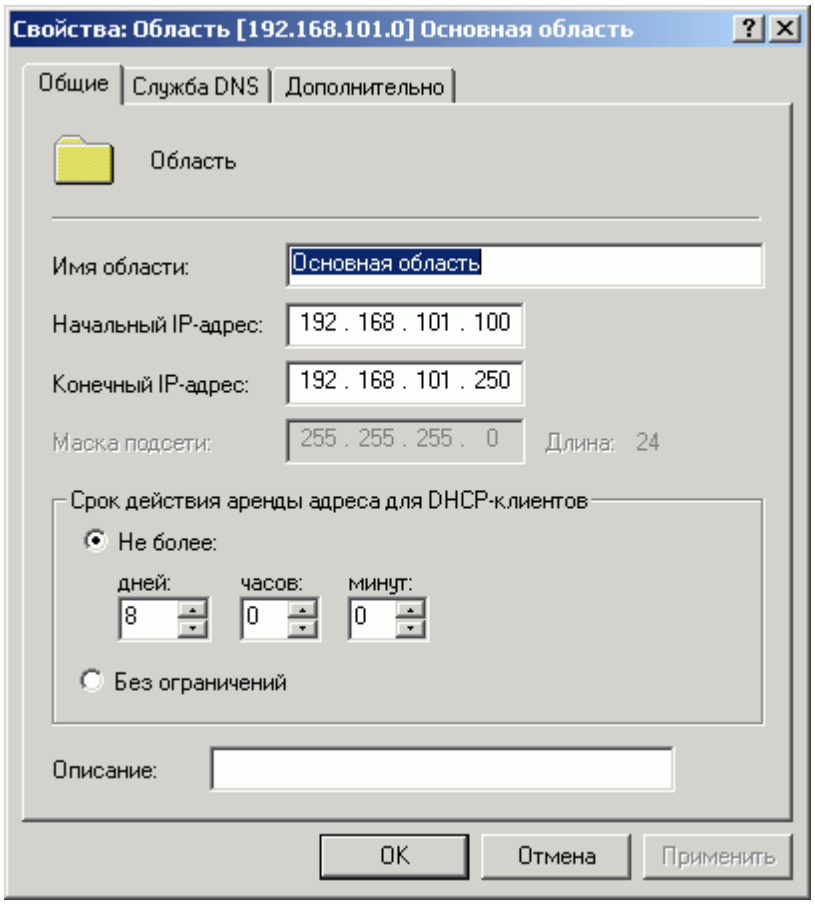
Управление службой DHCP

Изменение или просмотр свойств области

Чтобы открыть свойства области, запустите инструмент **DHCP**, в дереве консоли щелкните **сервер DHCP**, затем **требуемую область**. В меню **Действие** выберите команду **Свойства**.



Просмотрите и измените (если необходимо) свойства области. Для просмотра описания какого-либо элемента диалогового окна щелкните этот элемент правой кнопкой мыши и выберите команду **Что это такое?**



- Идентификаторы подсети и пул адресов (определяется значениями начального и конечного IP-адресов, использованными для создания области) составляют основные свойства области. Можно изменить только некоторые свойства существующей области, например диапазоны исключения, резервирования клиентов, настроенные значения типов параметров или установки времени для аренды адресов клиентами в области.
- Нельзя исключить диапазон адресов, включающий активную аренду. Сначала необходимо удалить активную аренду, а затем повторить исключение.
- Диапазон адресов области может быть расширен, но не может быть уменьшен. Однако в любое время можно исключить нежелательные адреса из полного диапазона адресов области.

Управление арендой адресов

IP-адреса предоставляются сервером DHCP в аренду его клиентам. Каждая аренда имеет срок

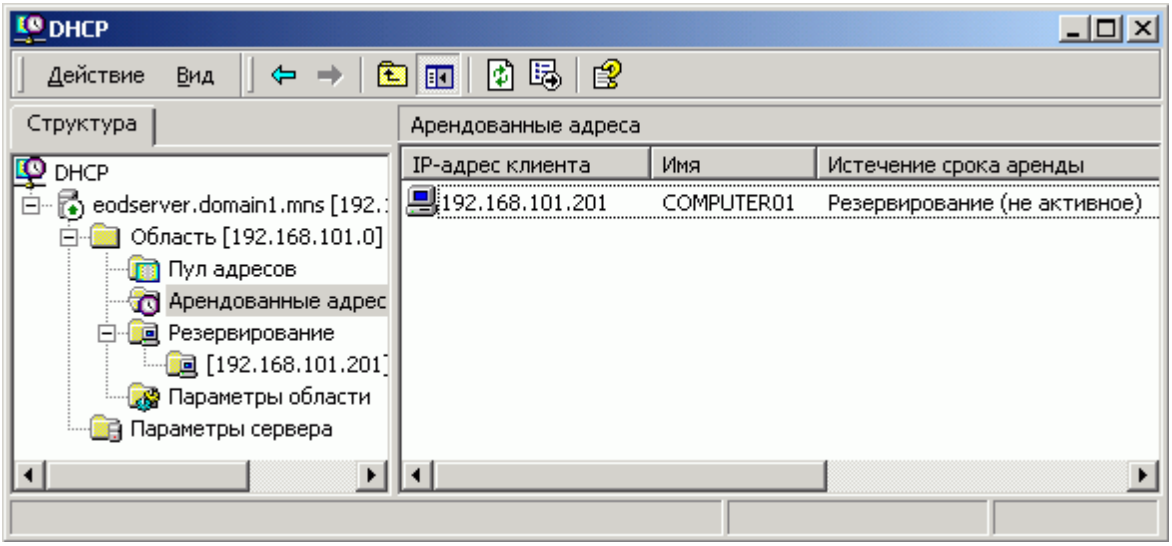
действия, по окончании которого клиент должен обновить аренду для дальнейшего использования того же адреса.

Сведения об аренде хранятся в базе данных сервера DHCP около суток после окончания срока действия аренды. Это позволяет сохранить аренду в случае, если клиент и сервер находятся в разных часовых поясах, а часы соответствующих компьютеров не синхронизированы, либо если во время окончания аренды клиентский компьютер отключен от сети. Истекшие аренды входят в список активных, но их значки затемнены.

Аренда любого клиента DHCP в рамках области может быть аннулирована. Обычно это необходимо, чтобы воспользоваться арендованным IP-адресом для статической (ручной) выдачи узлу или резервированием этого адреса за конкретно указанным узлом. Удаление аренды имеет такой же эффект, как и окончание срока действия: при следующей загрузке компьютер должен перейти в состояние инициализации и получить с сервера DHCP новые сведения о конфигурации TCP/IP. Единственный способ предотвратить повторное получение клиентом того же IP-адреса - перед запросом новой аренды клиентом вручную сделать адрес недоступным.

Следует аннулировать только записи клиентов, которые не используют назначенную аренду DHCP или требуют немедленного перемещения на новый адрес. Удаление аренды активного клиента может привести к дублированию IP-адресов в сети, поскольку удаленные адреса будут назначены новым активным клиентам. После удаления аренды клиента и настройки резервирования или исключения следует выполнять на клиентском компьютере команду **ipconfig /release** для принудительного освобождения IP-адреса.

Для просмотра сведений о текущей аренде следует выбрать в консоли **DHCP** папку **Арендованные адреса**. При этом в области сведений появится список арендованных в настоящее время адресов из данной области.



Изменение стандартной продолжительности аренды для области

При создании области по умолчанию устанавливается продолжительность аренды в восемь дней. Процесс обновления аренды происходит постоянно и может сказаться на быстродействии клиентов DHCP и сети, поэтому продолжительность аренды иногда полезно изменять. Для определения оптимальной продолжительности аренды с целью повышения производительности DHCP в сети используйте следующие рекомендации:

- При наличии в сети большого количества доступных IP-адресов и конфигураций, которые редко изменяются, увеличьте продолжительность аренды для снижения потока запросов на обновление между клиентами и сервером DHCP. Это уменьшит сетевой трафик, вызываемый процессами обновления аренды клиентами.

- При наличии ограниченного числа доступных IP-адресов, а также если в сети часто изменяются настройки или расположение клиентов, сократите продолжительность аренды для более быстрого освобождения неиспользуемых IP-адресов сервером DHCP. Это повысит частоту возвращения адресов в пул доступных адресов для назначения новым клиентам.

Резервирование адресов

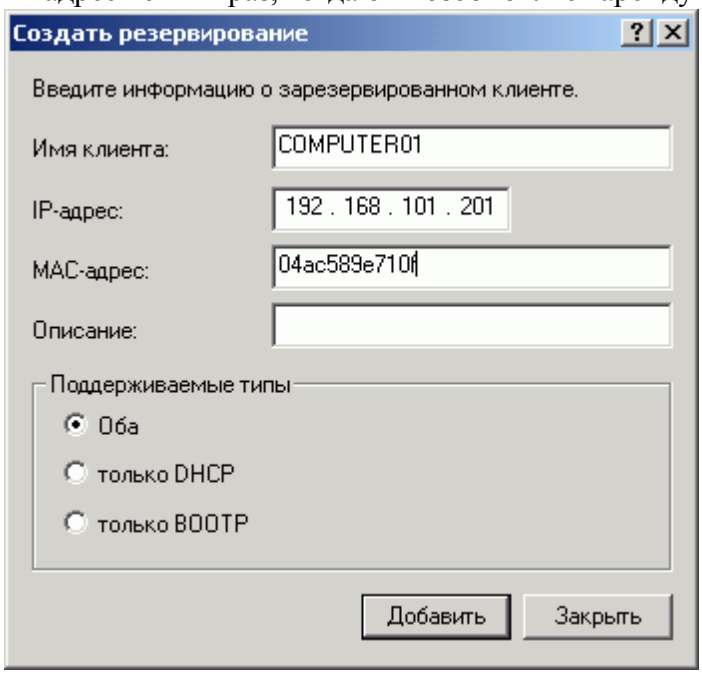
С помощью резервирования адресов у клиента есть возможность зарезервировать определенный IP-адрес для постоянного использования.

Если резервируется IP-адрес для нового клиента или адрес отличается от текущего значения, следует проверить, что адрес уже не был арендован DHCP-сервером. Резервирование для уже арендованного IP-адреса не вынуждает клиента, использующего этот адрес, прекратить аренду адреса.

Резервирование IP-адреса также не вынуждает нового клиента, для которого оно было выполнено, немедленно перейти на этот адрес. В этом случае на компьютере-клиенте, работающем под управлением Windows 2000, необходимо выполнить команду **ipconfig /renew**.

Для клиентов, использующих Windows 95 или Windows 98, можно использовать программу Winipcfg.exe, чтобы освободить или обновить зарезервированный IP-адрес в службе DHCP. Для клиентов, использующих MS-DOS, и некоторых клиентов, использующих другие операционные системы, для вступления изменений в силу компьютер должен быть перезапущен.

После внесения изменений клиент арендует зарезервированный для постоянного использования IP-адрес всякий раз, когда он возобновляет аренду на DHCP-сервере.



Удаление областей

Когда подсеть больше не используется или если по другой причине необходимо удалить существующую область, удаление производится в консоли DHCP. В большинстве случаев области удаляются, если необходимо полностью изменить один диапазон IP-адресов подсети на другой.

Чтобы изъять из обращения текущую область и перенастроить сеть на использования другой области, выполните нижеперечисленные действия:

1. Создайте новую область с помощью другого диапазона адресов.
2. Настройте параметры новой области.

3. Активизируйте новую область и отключите старую область.
4. Когда все клиенты перестанут использовать старую область, удалите ее.

Перед удалением области необходимо на некоторое время отключить ее. Отключение области запускает отзыв аренды в выбранной области.

Перед тем как отключить область, в сети должна быть активизирована область замещения. Область замещения может находиться на DHCP-сервере, отличном от того, на котором располагалась отключенная область, при условии, что область замещения располагается в той же подсети.

Перед удалением области она должна быть отключена. Это позволяет клиентам, использующим область, обновить аренду в другой области. В противном случае клиенты потеряют аренду. Если какой-либо IP-адрес в области по-прежнему арендован или используется, необходимо оставить область активной до тех пор, пока не истечет срок аренды или не будет отвергнут запрос клиента на обновление аренды.

После того как область отключена, она не распознает запросы аренды и обновления, поэтому существующие клиенты теряют свои аренды во время обновления и перенастраиваются на другой доступный DHCP-сервер. Чтобы гарантировать плавный переход всех клиентов на новую область, следует отключить старую область на время, равное по крайней мере половине времени аренды, или до того момента, когда все клиенты не будут обновлены вручную.

Чтобы вручную форсировать смену IP-адреса на компьютере под управлением Windows 2000, введите в командной строке на клиенте **ipconfig /release** или **ipconfig /renew**. Для других операционных систем может понадобиться перезагрузка компьютера-клиента.

Упражнение 4.А: "Установка и настройка службы DHCP"

Краткое описание

В этом упражнении Вы научитесь устанавливать и настраивать на сервере службу DHCP.

Предварительные требования к выполнению упражнения

Вам нужно самостоятельно установить Windows 2000 Server, чтобы выполнить эту и последующие работы в темах 4 и 6. Предполагается, что навыки установки сервера Вы получили в результате прослушивания очных курсов.

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права администратора.
2. Последовательно выберите **Пуск**, **Настройка**, **Панель управления**, **Установка и удаление программ**.
3. В окне **Установка и удаление программ** выберите **Добавление и удаление компонентов Windows**.
4. На странице **Мастер компонентов Windows** выберите пункт **Сетевые службы** и нажмите **Состав...**.
5. На странице **Сетевые службы** отметьте флажок **DHCP** и нажмите **ОК**. Нажмите **Далее**, чтобы продолжить установку службы.
6. Если **Мастер компонентов Windows** запросит файлы из дистрибутива Windows 2000, вставьте в CD-дисковод компакт-диск с дистрибутивом Windows 2000 Server и укажите путь к требуемым файлам.
7. На странице **Завершение работы мастера компонентов Windows** нажмите **Готово**.
8. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **DHCP**
9. Чтобы авторизовать сервер в Active Directory (если она установлена на сервере), щелкните правой кнопкой мыши на сервере и выберите **Авторизовать**. Подождите несколько минут, чтобы авторизация вступила в действие.
10. Щелкните правой кнопкой мыши на сервере и выберите **Создать область...**. Нажмите **Далее** на странице **Вас приветствует мастер создания области**.
11. На странице **Имя области** в поле **Имя** введите ***2 этаж***, нажмите **Далее**.
12. На странице **Диапазон адресов** введите **Начальный IP-адрес** - ***192.168.105.10***, а **Конечный IP-адрес** - ***192.168.105.100***. Нажмите **Далее**.
13. На странице **Добавление исключений** нажмите **Далее**, чтобы не настраивать исключения.
14. На странице **Срок действия аренды адресы** нажмите **Далее**, чтобы оставить срок аренды по умолчанию - 8 дней.
15. На странице **Настройка параметров DHCP** выберите **Да, настроить эти параметры сейчас** и нажмите **Далее**.
16. На странице **Маршрутизатор (основной шлюз)** введите в поле **IP-адрес** значение ***192.168.105.1*** ,нажмите **Добавить** и **Далее**.
17. На странице **Имя домена и DNS-серверы** введите в поле **Родительский домен** строку

domain1.local, а в поле **IP-адрес** значение ***192.168.105.5***. Нажмите **Добавить** и **Далее**

18. На странице **WINS-серверы** нажмите **Далее**, чтобы не настраивать работу с WINS-серверами.
19. На странице **Активизировать область** выберите **Да, я хочу активизировать эту область сейчас**.
20. На странице **Завершение работы мастера создания области** нажмите **Готово**.
21. Щелкните правой кнопкой мыши на созданной области, выберите **Свойства**. Проверьте, что установленные параметры соответствуют заданным ранее в пунктах 11, 12 и 14.

Занятие 3: "Разрешение имен"

Протокол IP работает с 32-битными IP-адресами узла-источника и узла-приемника, но с компьютерами работают люди, которым трудно запоминать цифровые IP-адреса. Если имя используется, как псевдоним IP-адреса, то необходимо обеспечить уникальность этого имени и связать его с соответствующим IP-адресом. Аналогией является телефонный справочник. Фамилию человека или название организации запомнить намного проще, чем семизначный телефон.

В Windows 2000 поддерживаются два типа имен, которые могут разрешаться в IP-адреса.

- **Имена узлов**

  Имена узлов применяются в программах, использующих интерфейс программирования Windows Sockets, например в веб-обозревателях.
- **Имена NetBIOS**

  Имена NetBIOS применяются в сетевых программах и службах, использующих интерфейс программирования NetBIOS, например в клиенте для сетей Microsoft и в службе доступа к файлам и принтерам сетей Microsoft.

Разрешение имен узлов

Разрешение имени узла — это процесс определения IP-адреса узла по его имени. Имя узла представляет собой псевдоним, присваиваемый IP-узлу и идентифицирующий его в TCP/IP-сети. Имя узла может быть длиной до 255 символов и содержать алфавитно-цифровые символы, дефисы и точки. Одному узлу можно присвоить несколько имен узлов.

Программы Windows Sockets (Winsock), например Internet Explorer и служебная программа FTP, могут использовать для обозначения узла, к которому выполняется подключение, любое из двух значений: IP-адрес или имя узла. Если используется IP-адрес, то необходимость в разрешении имени отпадает. Если же указывается имя узла, то для установления IP-соединения с нужным ресурсом нужно сначала разрешить имя узла в IP-адрес.

Имена узлов могут иметь различные формы. Две наиболее популярных формы — короткое имя и полное (доменное) имя. Короткое имя — это псевдоним IP-адреса, который могут назначать отдельные пользователи. Полное имя — это структурированное имя в иерархическом пространстве имен, называемом ***системой доменных имен*** (Domain Name System — DNS). Примером доменного имени является www.microinform.ru, а коротким именем в данном случае будет www.

Короткие имена разрешаются с помощью записей в файле **WINNT\System32\Drivers\Etc\Hosts**.

Полные имена разрешаются путем отправки DNS-запроса соответствующему DNS-серверу. DNS-сервер — это компьютер, хранящий записи, сопоставляющие имена доменов и IP-адреса, или умеющий обращаться к другим DNS-серверам. DNS-сервер разрешает доменное имя в IP-адрес и возвращает результат разрешения.

Для разрешения доменных имен на компьютере Windows 2000 нужно задать IP-адрес DNS-сервера. На компьютерах Windows 2000 для корректного использования службы каталогов Active Directory необходимо задать IP-адрес DNS-сервера.

Разрешение имен NetBIOS

Разрешение имени NetBIOS — это процесс определения IP-адреса по имени NetBIOS. Имя NetBIOS представляет собой 16-байтовый адрес, используемый для идентификации в сети ресурса NetBIOS. Имя NetBIOS может быть уникальным или групповым. Когда процесс NetBIOS соединяется с конкретным процессом на конкретном компьютере, используется уникальное имя. Когда процесс NetBIOS соединяется с несколькими процессами на нескольких компьютерах, применяется групповое имя.

Служба доступа к файлам и принтерам сетей Microsoft, работающая на компьютере с Windows 2000 - пример процесса, использующего имя NetBIOS. При запуске компьютера эта служба регистрирует уникальное имя NetBIOS, основанное на имени компьютера. Для этой службы имя NetBIOS состоит из 15-символьного имени компьютера плюс 16-й символ с кодом 0x20. Если имя компьютера имеет длину меньше 15 символов, оно дополняется до этой длины пробелами. Пример: **MOSCOW** или **HPLJ4P**. Для просмотра имен NetBIOS можно воспользоваться командами net view и nbtstat -c.

Имена NetBIOS широко использовались в сетях на основе DOS и более ранних версий Windows. В наше время имена NetBIOS используются реже и вытесняются именами узлов. Поэтому в данном курсе рассматриваются только имена узлов и использующая их служба DNS.

Занятие 4: "Служба доменных имен DNS"

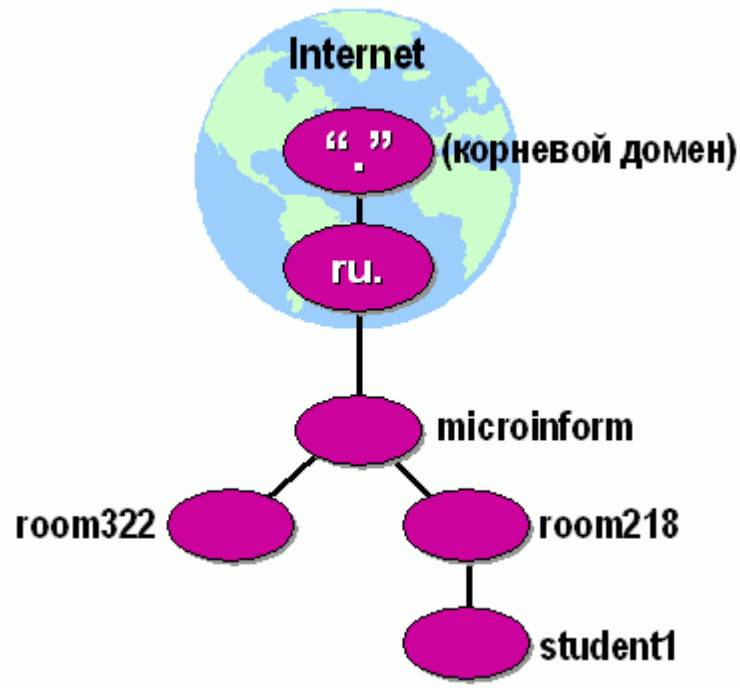
Вводные сведения о DNS

Служба доменных имен DNS является стандартной службой имен Интернета и TCP/IP. ***DNS*** - аббревиатура от Domain Name System (система доменных имен), т.е. системы наименования компьютеров и сетевых служб, организованных в виде иерархии доменов. Правила наименования DNS используются в сетях TCP/IP, таких как Интернет, для поиска компьютеров и служб по именам. Задача службы DNS - сопоставить введенное пользователем в приложении имя DNS с IP-адресом.

Большинство пользователей предпочитает использовать для обращения к почтовому серверу или веб-серверу в Интернете имя, такое как www.microinform.ru или www.microsoft.com. Компьютеры при связи по сети используют числовые адреса. Для упрощения работы с сетевыми ресурсов, службы имен, такие как DNS, обеспечивают сопоставление понятного имени компьютера или службы с его числовым адресом. Например, Вы используете DNS, работая с веб-обозревателем.

Общие сведения о пространстве доменных имен DNS

Пространство доменных имен DNS базируется на концепции дерева именованных доменов (см. рисунок ниже). Каждый уровень дерева может представлять ветвь или лист дерева. Ветвь представляет уровень, на котором используется несколько имен, определяющих семейство именованных ресурсов. Лист представляет единственное имя, которое используется на этом уровне для указания конкретного ресурса.



Организация пространства доменных имен DNS

Любое доменное имя DNS в дереве технически представляет домен. Однако в большинстве дискуссий

DNS имена идентифицируются одним из пяти способов на основании уровня и способа использования имени. Например, доменное имя DNS, зарегистрированное для компании МИКРОИНФОРМ (microinform.ru.), представляет домен второго уровня. Это имя состоит из двух частей (называемых метками), показывающих, что оно находится на втором уровне сверху от корня или вершины дерева. Большинство доменных имен DNS содержат две или большее число меток, каждая из которых задает новый уровень в дереве. Точки используются в именах для разделения меток.

В следующей таблице представлен ряд терминов, используемых для описания доменных имен DNS по их функциям в пространстве имен.

Тип имени	**Описание**	**Пример**
Корневой домен	Вершина дерева, представляющая неименованный уровень; иногда обозначается парой прямых кавычек (""), указывающих пустое значение. При использовании в доменном имени DNS устанавливается с помощью завершающей точки (.), обозначающей, что имя расположено в корне или на самом верхнем уровне иерархии доменов. В данном случае доменное имя DNS рассматривается как полное и указывает на точное расположение в дереве имен. Имена, установленные таким способом, называют полными доменными именами (FQDN).	Единственная точка (.) или точка, использованная в конце имени, например, «example.microinform.ru.».
Домен верхнего уровня	Имя из двух или трех букв, которое используется, чтобы указать страну/регион или тип организации.	«.ru» указывает имя, зарегистрированное для использования организациями и гражданами России в Интернете.
Домен второго уровня	Имена переменной длины, зарегистрированные для индивидуальных пользователей или организаций для использования в Интернете. Они всегда базируются на соответствующем домене верхнего уровня в зависимости от типа организации или географического расположения.	«microinform.ru.» является именем домена второго уровня, зарегистрированным для компании МИКРОИНФОРМ регистратором доменных имен DNS Интернета.
Поддомен	Дополнительные имена, которые организация может создавать как производные от зарегистрированного имени домена второго уровня. Такие имена обеспечивают рост дерева имен DNS в организации и его распределение по отделам или по географическому расположению.	«room218.microinform.ru.» - имя несуществующего поддомена, предназначенного для примера.

Имя узла или ресурса	Имя, представляющее лист в дереве имен DNS, которое определяет конкретный ресурс. Обычно крайняя левая метка в доменном имени DNS определяет конкретный компьютер в сети. Например, имя этого уровня, используемое в записи ресурса узла (A), применяется для поиска IP-адреса компьютера по его имени узла.	«student1.room218.microinform.ru.», где первая метка («student1») представляет имя узла DNS для конкретного компьютера в сети.

Интерпретация доменного имени DNS

DNS представляет способ интерпретации полного пути к доменному имени DNS аналогично способу интерпретации полного пути к файлу или каталогу в окне командной строки.

Путь в дереве каталогов помогает указать на точное расположение сохраненного на компьютере файла. Для компьютеров с операционной системой Windows обратная косая черта (\) указывает очередной новый каталог, ведущий к точному расположению файла. Эквивалентным символом в DNS является точка (.), указывающая каждый новый уровень домена в имени.

Например, для файла с именем Services полный путь, отображаемый в окне командной строки Windows, может иметь вид:

```
C:\Winnt\System32\Drivers\Etc\Services
```

Для интерпретации полного пути к файлу имя читается слева направо от верхнего, т.е. наиболее общего уровня (диск C, т.е. диск, на котором сохранен файл) до конкретного имени файла «Services». Этот пример показывает пять уровней иерархии, ведущих к расположению файла Services на диске C.

1. Корневая папка диска C (C:\).
2. Системная папка Windows (Winnt).
3. Системная папка, в которой сохранены системные компоненты (System32).
4. Папка, в которой сохранены драйверы системных устройств (Drivers).
5. Папка, в которой сохранены различные файлы, используемые драйверами системных и сетевых устройств (Etc).

Для DNS примером имени с несколькими уровнями может служить следующее полное доменное имя узла:

```
student1.room218.microinform.ru.
```

В отличие от имен файлов, при чтении полного доменного имени узла DNS слева направо осуществляется переход от наиболее конкретной информации (имя DNS компьютера «student1») к наиболее общей (завершающая точка (.), которая указывает корень в дереве имен DNS). Этот пример демонстрирует четыре уровня доменов DNS, которые ведут от конкретного расположения «student1».

1. Домен «room218», в котором зарегистрировано для использования имя компьютера «student1».
2. Домен «microinform», который соответствует родительскому домену, являющемуся корнем поддомена «room218».
3. Домен «ru», который соответствует домену верхнего уровня, предназначенному для использования организациями и гражданами России, который является корнем для домена «microinform».
4. Завершающая точка (.), представляющая стандартный символ разделителя, которая используется, чтобы сделать полным доменное имя DNS в дереве пространства имен DNS.

Общие сведения о различии между зонами и доменами

Зона начинается как база данных для единственного доменного имени DNS. Если ниже уровнем используемого для создания зоны доменом добавляются другие домены, эти домены могут быть частью той же зоны или входить в другую зону. После добавления поддомена, он может:

- включаться и управляться как часть записей исходной зоны;
- делегироваться в другую зону, созданную для поддержки поддомена.

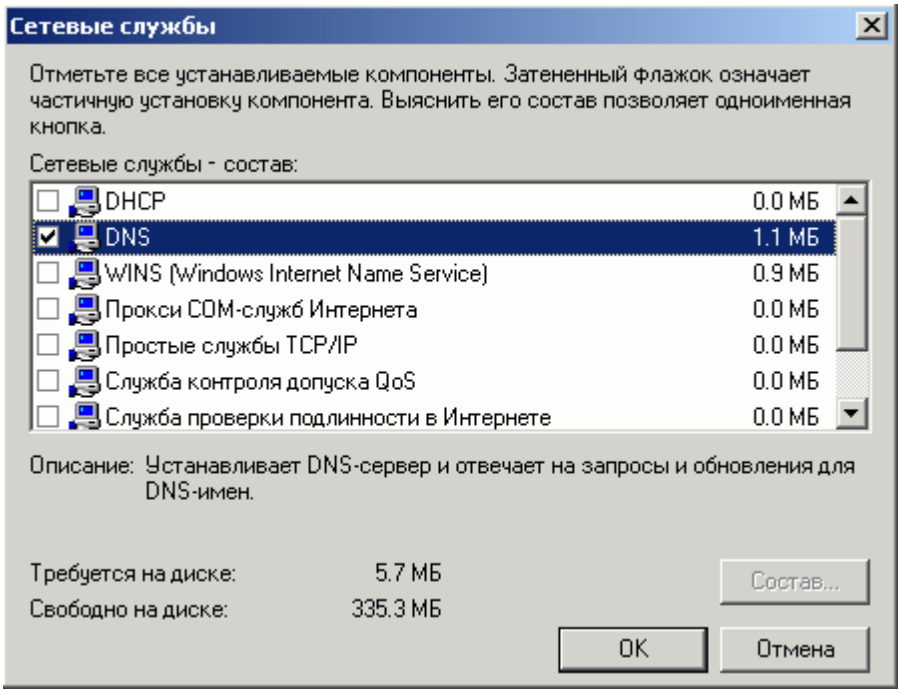
Занятие 5: "Реализация службы DNS в Windows 2000"

Служба доменных имен DNS является стандартной службой имен Интернета и TCP/IP. Эта служба позволяет компьютерам клиентов в сети регистрировать и сопоставлять доменные имена DNS. Эти имена используются для поиска и доступа к ресурсам, предлагаемым другими компьютерами в вашей сети или другими сетями, такими как Интернет.

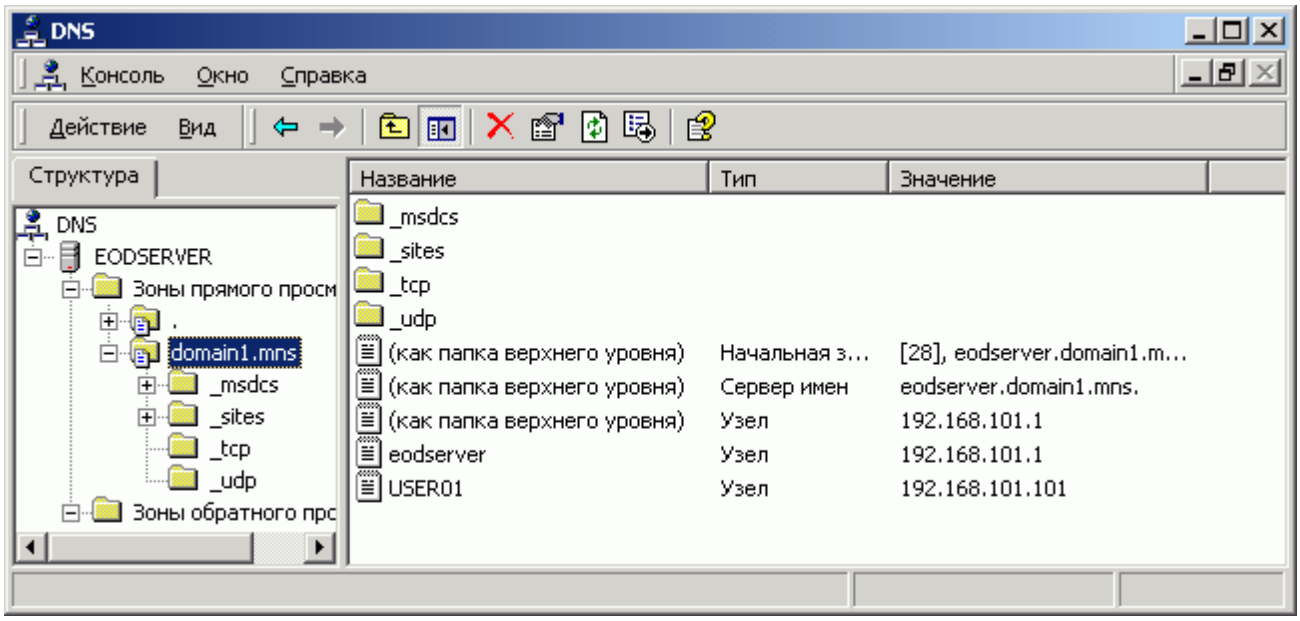
Основным инструментом управления DNS-серверами Windows 2000 является консоль **DNS**, доступная в папке **Администрирование** панели управления.

Порядок установки и настройки службы DNS

1. Определите, для чего будет использоваться служба DNS - для домена Интернета или домена Active Directory. Если домен создается для Active Directory, то необходимо повысить компьютер сервера до контроллера домена, чтобы установить DNS-сервер, а также автоматически создать и настроить необходимую для работы Active Directory зону. В противном случае установите службу DNS, добавив ее в **Мастере компонентов Windows**, в списке **Сетевые службы**.



2. Если при установке Active Directory зона не создалась, или мы используем DNS для домена Интернета, создайте зону для домена.
3. Создайте необходимые записи ресурсов (например, для веб-серверов).



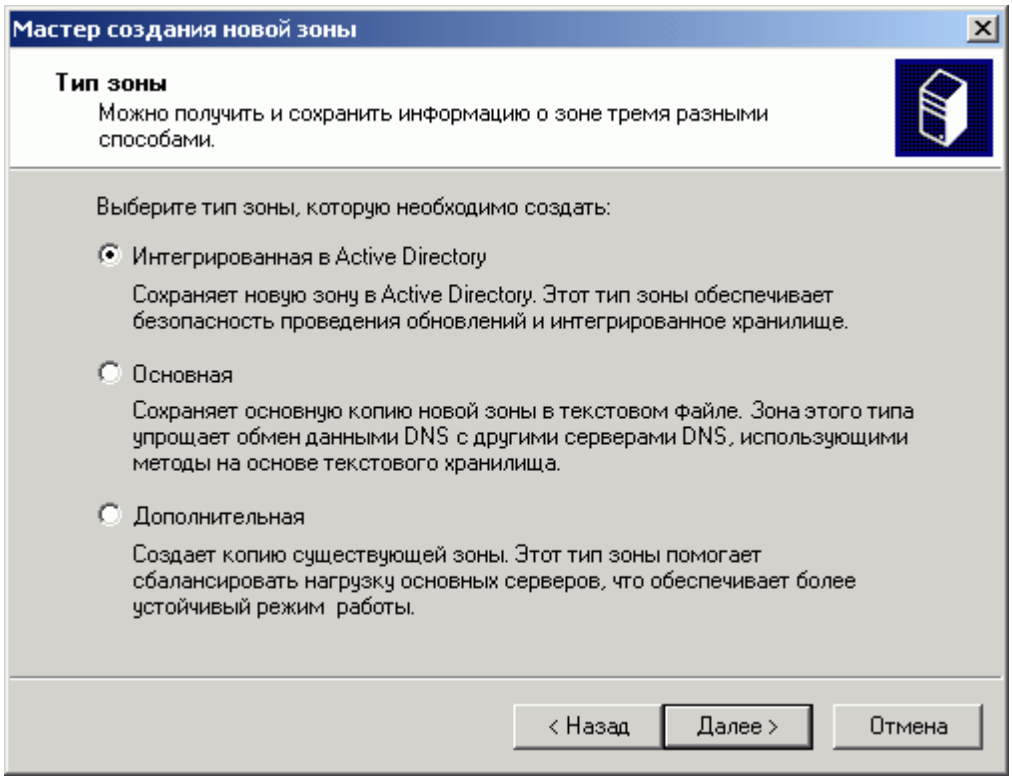
Создание зон прямого просмотра

Запустите инструмент "DNS". В дереве консоли щелкните **DNS**, **DNS-сервер**, **Зоны прямого просмотра**. В меню **Действие** выберите **Создать новую зону**.

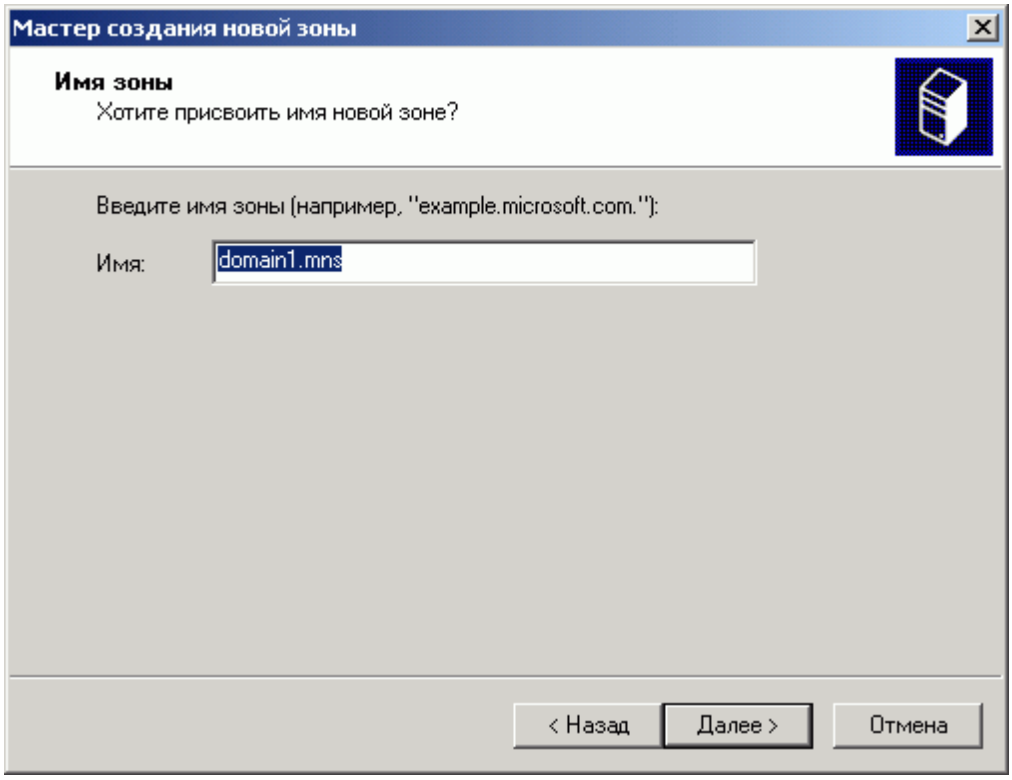
Выберите тип зоны для домена. При создании зоны для домена Интернета выберите **Основная**, если на этом сервере будет храниться единственная копия зоны, доступная для записи, и тогда этот DNS-сервер зоны считается источником изменений для зоны.

Если необходимо настроить DNS на хранение копии зоны и ее регулярное обновление, а оригинал зоны находится, например, у Интернет-провайдера, выберите **Дополнительная**.

Тип зоны **Интегрированная в Active Directory** будет доступен, только если DNS-сервер также является контроллером домена. Рекомендуется выбирать этот тип зоны только для доменов DNS в локальной сети и, в первую очередь, для зон доменов Active Directory.



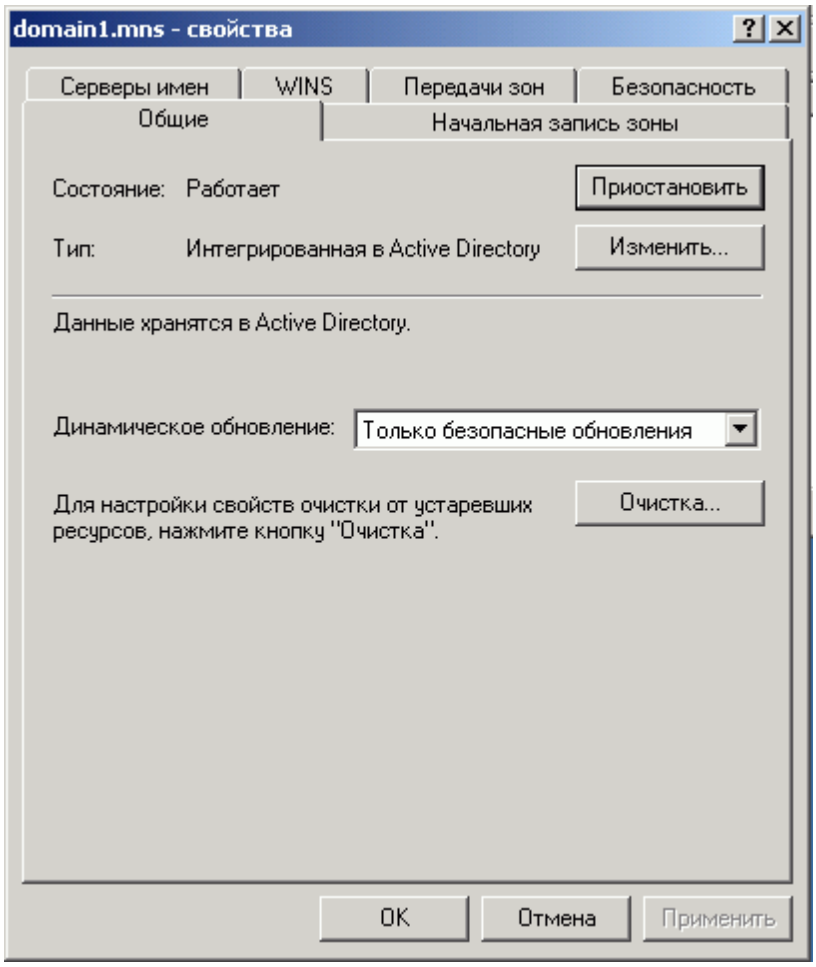
Введите имя домена. Для доменов Active Directory можно использовать любые именования доменов, но для доменов Интернета нужно использовать только зарегистрированные имена доменов.



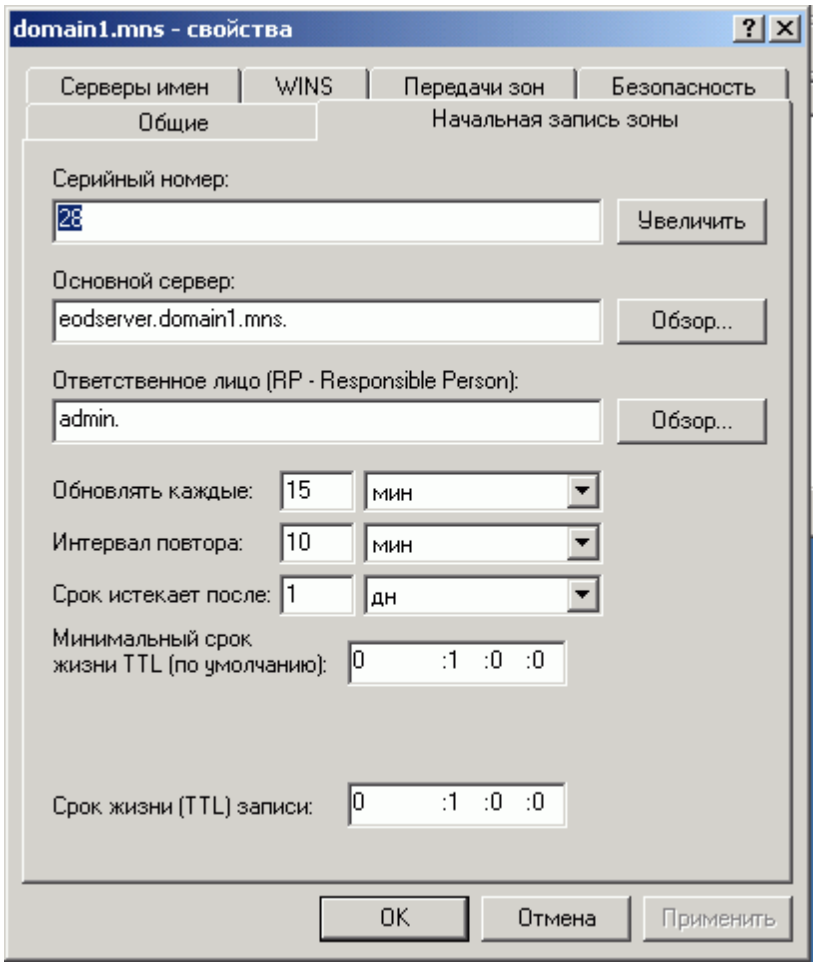
Изменение свойств зоны

Основные настройки зоны находятся на закладках **Общие**, **Начальная запись зоны** и **Передача зон**.

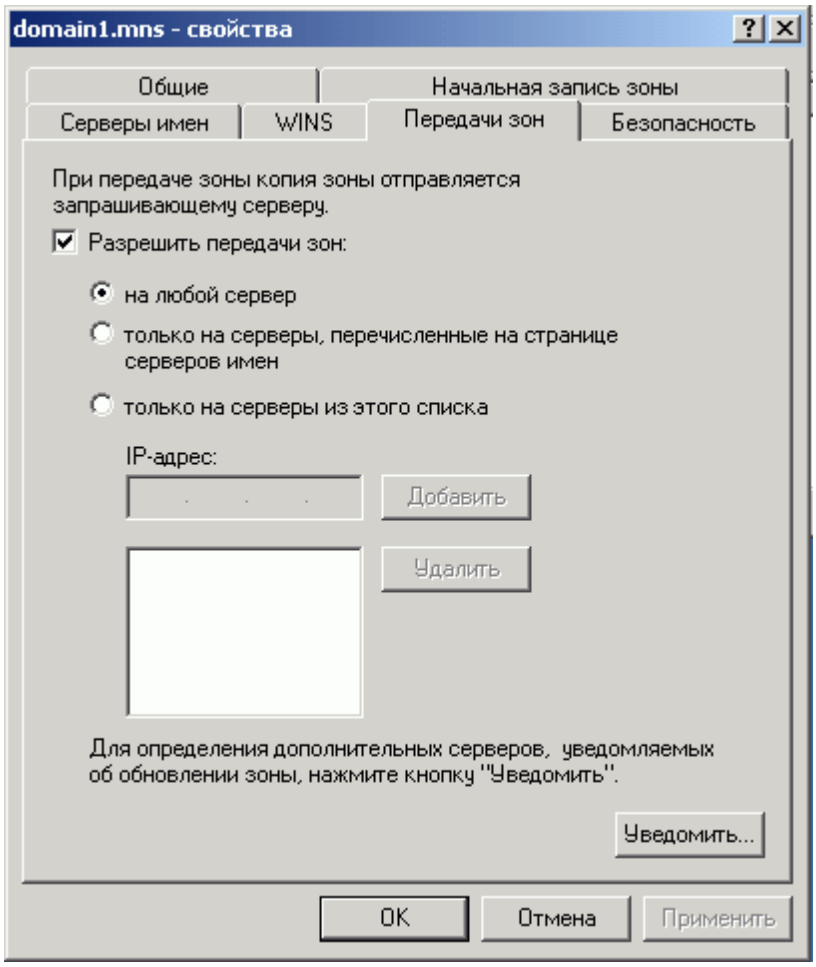
На закладке **Общие** можно изменить тип зоны (например, с **Основная** в **Интегрированная в Active Directory**), приостановить или запустить обслуживание сервером зоны, отключить или включить динамического обновление зоны. Для зон, интегрированных в службу каталогов, можно включить использование только безопасных обновлений. Это позволяет ограничить обновления только набором авторизованных пользователей или компьютеров. Когда для зоны включены безопасные обновления, только пользователям, компьютерам или группам, авторизованным через службу каталогов Active Directory и включенным в список управления доступом (ACL) для каждой интегрированной зоны, разрешается обновлять зону или используемые в ней специфические записи ресурсов.



На закладке **Начальная запись зоны** можно настроить свойства ***начальной записи зоны***, которая используется для инициализации зоны и указывает полномочия зоны для доменного имени DNS (вместе с любыми поддоменами, не делегированными на другие серверы) для других членов пространства имен DNS. Эта запись определяет, как часто зона должна обновляться и передаваться другим серверам, хранящим эту зону, а также сроки кэширования записей ресурсов при возвращении ответов на запросы имен в зоне.



На закладке **Передача зон** необходимо ограничить передачу зоны только на те сервера, которые участвуют в ее обслуживании - разрешить передачи только на DNS-серверы, заданные на вкладке **Серверы имен** или только на DNS-серверы, указанные по IP-адресам в списке.



Добавление и обновление записей ресурсов

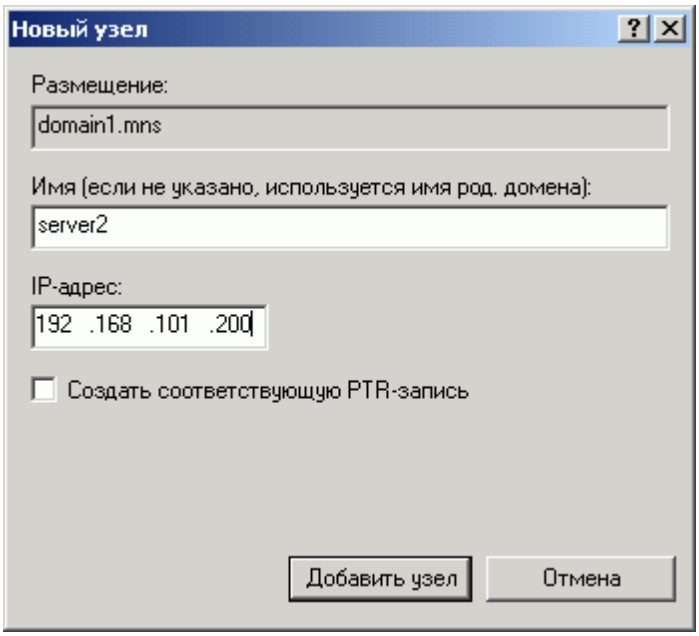
После создания зоны в нее следует добавить дополнительные записи ресурсов. Обычно добавляются следующие записи ресурсов.

- Узел (A) Для сопоставления доменного имени DNS с IP-адресом, используемым компьютером.
- Псевдоним (CNAME) Для сопоставления псевдонима доменного имени DNS с другим первичным или каноническим именем.
- Почтовый обменник (MX) Для сопоставления доменного имени DNS с именем компьютера, который выполняет обмен или перенаправление почты.
- Расположение службы (SRV) Для сопоставления доменного имени DNS с указанным списком узлов DNS, предлагающих определенный тип службы, например, с контроллерами домена службы каталогов Active Directory.

Записи ресурсов узлов (A)

Записи ресурсов имен узлов (**A**) используются в зоне для связывания доменных имен DNS компьютеров (узлов) с их IP-адресаами. Эти записи могут добавляться в зону несколькими способами.

- Можно создать запись ресурса для компьютера, использующего статическую IP-адресацию, с помощью консоли DNS. Для этого правой кнопкой щелкните на зоне и выберите **Создать узел...**.



- Компьютеры, выполняющие Windows 2000, используют службу DHCP-клиент для динамической регистрации и обновления собственных записей ресурсов **A** в DNS, когда конфигурация IP изменяется.
- Для клиентских компьютеров с включенной службой DHCP, на которых выполняются предыдущие версии операционных систем корпорации Майкрософт, записи ресурсов **A** регистрируются и обновляются DHCP-сервером, если эти компьютеры получают аренду IP от квалифицированного DHCP-сервера.

Записи ресурсов (**A**) не являются обязательными для всех компьютеров, но они необходимы для совместно использующих ресурсы в сети компьютеров. Любой компьютер, совместно использующий ресурсы в сети, который должен идентифицироваться по своему доменному имени DNS, нуждается в записях ресурсов **A**, которые обеспечивают сопоставление имени DNS с IP-адресом компьютера.

Большая часть записей ресурсов **A**, требуемых в зоне, может относиться к другим рабочим станциям и серверам, содержащим общие ресурсы, другим DNS-серверам, почтовым серверам и веб-серверам. Такие записи ресурсов представляют большинство записей ресурсов в базе данных зоны.

Записи ресурсов псевдонимов (CNAME)

Записи ресурсов псевдонимов (**CNAME**) иногда называют *каноническими именами*. Такие записи позволяют использовать несколько имен для указания на один узел, что облегчает одновременное использование одного компьютера в качестве FTP-сервера и веб-сервера. Например, общеизвестные имена сервера (**ftp**, **www**) регистрируются с помощью записей ресурсов **CNAME**, которые обеспечивают сопоставление с именем узла DNS, таким как **server-2**, для компьютера, на котором выполняются эти службы.

Использование записей ресурсов **CNAME** рекомендуется в следующих ситуациях.

- Когда необходимо переименовать узел, указанный в записи ресурса **A** в той же зоне.
- Когда универсальное имя общеизвестного сервера, такое как **www**, должно быть сопоставлено группе отдельных компьютеров (каждому из которых соответствует отдельная запись ресурса **A**), обеспечивающих одну и ту же службу. Например, группе избыточных веб-серверов.

При переименовании компьютера с существующей записью ресурса **A** в зоне имеется возможность использовать временную запись ресурса **CNAME**, чтобы предоставить пользователям и программам отсрочку для переключения от использования старого имени компьютера к использованию нового имени. Для этого требуются следующие действия.

- Для нового доменного имени DNS компьютера в зону добавляется новая запись ресурса **A**.
- Для старого доменного имени DNS добавляется запись ресурса **CNAME**, указывающая на

новую запись ресурса **A**.
- Исходная запись ресурса **A** для старого доменного имени DNS удаляется из зоны.

Когда запись ресурса **CNAME** используется для создания псевдонима или переименования компьютера, следует задать лимит времени на использование этой записи в зоне перед ее удалением из DNS. Если пользователь забывает удалить запись ресурса **CNAME**, а затем удаляется соответствующая запись ресурса **A**, наличие записи **CNAME** может привести к напрасному расходованию ресурсов сервера на попытки сопоставления в запросах имени, которое больше не используется в сети.

Обычно и чаще всего запись ресурса **CNAME** требуется для создания постоянного псевдонима доменного имени DNS при сопоставлении универсальных имен, базирующихся на имени службы, таких как **www.domain1.mns**, нескольким компьютерам или IP-адресам, используемым на веб-сервере. Например, ниже демонстрируется общий синтаксис использования записи ресурса **CNAME**.

псевдоним **IN CNAME** *первичное_каноническое_имя*

В этом примере компьютер с именем **server2.domain1.mns** должен работать одновременно как веб-сервер с именем **www.domain1.mns** и FTP-сервер с именем **ftp.domain1.mns**. Чтобы обеспечить требуемое наименование компьютера, можно добавить и использовать следующие записи **CNAME** в зоне **domain1.mns**:

```
server2   IN  A      10.0.0.22
ftp       IN  CNAME  server2
www       IN  CNAME  server2
```

Если в дальнейшем потребуется перевести FTP-сервер на другой компьютер, отличный от веб-сервера на компьютере **server2**, просто измените запись ресурса CNAME в зоне для ftp.domain1.mns и добавьте дополнительную запись ресурса A в зону для нового компьютера, на котором будет выполняться FTP-сервер.

На основании предыдущего примера, если имя нового компьютера **server1.domain1.mns**, новая и измененная записи ресурсов A и CNAME будут иметь вид:

```
server1   IN  A      10.0.0.21
server2   IN  A      10.0.0.22
ftp       IN  CNAME  server2
www       IN  CNAME  server1
```

Записи ресурсов почтового обменника (MX)

Запись ресурса почтового обменника (**MX**) используется приложениями электронной почты для обнаружения почтового сервера по доменному имени DNS, используемому в адресе получателя сообщения электронной почты. Например, запрос DNS к имени **domain1.mns** может использоваться для поиска записи ресурса **MX**, что позволит приложению электронной почты направлять или обмениваться сообщениями с пользователем, имеющим почтовый адрес **user@domain1.mns**.

Запись ресурса **MX** показывает доменное имя DNS для компьютера или компьютеров, которые обрабатывают почту для домена. Если существуют несколько записей ресурсов MX, служба DNS-клиент пытается установить связь с почтовыми серверами в порядке указанного предпочтения, от минимального значения (высший приоритет) к максимальному (низший приоритет). Ниже приводится пример основного синтаксис при использовании записи ресурса **MX**.

почтовое_доменное_имя **IN MX** *предпочтение узел_почтового_сервера*

С помощью записей ресурсов **MX**, показанных ниже для зоны **domain1.mns**, почта с адресом **user@domain1.mns** будет, по возможности, доставлена на адрес **user@mailserver0.domain1.mns**. Если этот сервер недоступен, клиент службы сопоставления имен может использовать адрес **user@mailserver1.domain1.mns**.

```
@          IN  MX   1    mailserver0
@          IN  MX   2    mailserver1
```

Следует отметить, что использование символа (**@**) в записях указывает, что доменное имя DNS отправляющего совпадает с исходным именем зоны (**domain1.mns**).

Записи ресурсов размещения службы (SRV)

Чтобы обнаружить контроллеры домена службы каталогов Active Directory в Windows 2000, требуются записи ресурсов расположения службы (SRV). Обычно при установке службы каталогов Active Directory нет необходимости вручную администрировать записи ресурсов **SRV**.

Мастер установки службы каталогов Active Directory по умолчанию пытается обнаружить DNS-сервер по списку основных или дополнительных DNS-серверов, указанных в свойствах клиента TCP/IP для каждого из его активных сетевых подключений. Если выполняется соединение с DNS-сервером, который может принимать динамическое обновление записи ресурса **SRV** (и других записей ресурсов, относящихся к регистрации Active Directory как службы в DNS), то процесс задания конфигурации завершается.

Если во время установки не обнаруживается DNS-сервер, который может принимать обновления для выбранного имени домена, то DNS-сервер Windows 2000 может быть установлен локально и автоматически настроен с зоной, базирующейся на домене службы каталогов Active Directory.

Например, если доменом Active Directory, выбранным в качестве первого домена в лесу, является **domain1.mns**, будет добавлена зона с корневым доменным именем DNS **domain1.mns**. Эта зона будет настроена на использование с DNS-сервером, выполняющемся на новом контроллере домена.

Если не установить DNS-сервер, встроенный в Windows 2000, то в процессе установки службы каталогов Active Directory создается и записывается файл (Netlogon.dns), содержащий записи ресурсов **SRV** и другие записи ресурсов, требуемые для поддержки Active Directory. Этот файл создается в папке %SystemRoot%\System32\Config.

Если используется DNS-сервер, отвечающий одному из следующих описаний, необходим использовать записи в файле Netlogon.dns, чтобы вручную настроить основную зону на сервере для поддержки службы каталогов Active Directory.

1. Компьютер, работающий как DNS-сервер, выполняет другую операционную систему, такую как UNIX, и не может распознавать или принимать динамические обновления.
2. DNS-сервер на этом компьютере является полномочным для основной зоны, соответствующей доменному имени DNS домена службы каталогов Active Directory.
3. DNS-сервер поддерживает записи ресурсов SRV, но не поддерживает динамические обновления. Например, служба DNS, обеспечиваемая Windows NT Server 4.0, после обновления до Service Pack 4 или более поздней версии удовлетворяет этому описанию.

Упражнение 4.Б: "Установка и настройка службы DNS"

Краткое описание

В этом упражнении Вы научитесь устанавливать и настраивать на сервере службу DNS.

Предварительные требования к выполнению упражнения

Вам нужно самостоятельно установить Windows 2000 Server, чтобы выполнить эту и последующие работы в темах 4 и 6. Предполагается, что навыки установки сервера Вы получили в результате прослушивания очных курсов.

Порядок выполнения упражнения

1. Войдите в операционную систему под учетной записью пользователя, имеющего права администратора.
2. Последовательно выберите **Пуск**, **Настройка**, **Панель управления**, **Установка и удаление программ**.
3. В окне **Установка и удаление программ** выберите **Добавление и удаление компонентов Windows**.
4. На странице **Мастер компонентов Windows** выберите пункт **Сетевые службы** и нажмите **Состав...**.
5. На странице **Сетевые службы** отметьте флажок **DNS** и нажмите **ОК**. Нажмите **Далее**, чтобы продолжить установку службы.
6. Если **Мастер компонентов Windows** запросит файлы из дистрибутива Windows 2000, вставьте в CD-дисковод компакт-диск с дистрибутивом Windows 2000 Server и укажите путь к требуемым файлам.
7. На странице **Завершение работы мастера компонентов Windows** нажмите **Готово**.
8. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **DNS**
9. В дереве консоли щелкните **DNS**, **DNS-сервер**, **Зоны прямого просмотра**. В меню **Действие** выберите **Создать новую зону**.
10. На странице **Вас приветствует мастер создания новой зоны** нажмите **Далее**.
11. На странице **Тип зоны** выберите **Основная**, нажмите **Далее**.
12. На странице **Имя зоны** в поле **Имя** введите ***domain1.local***, нажмите **Далее**.
13. На странице **Файл зоны** нажмите **Далее**, чтобы оставить имя файла зоны по умолчанию.
14. На странице **Завершение работы мастера создания новой зоны** нажмите **Готово**.
15. Щелкните правой кнопкой мыши на зоне **domain1.local** и выберите **Создать узел...**
16. В окне **Новый узел** введите в поле **Имя** значение ***testserver1***, а в поле **IP-адрес** - ***192.168.105.7***. Нажмите **Добавить узел**, **ОК**, а затем **Готово**.
17. Щелкните правой кнопкой мыши на зоне **domain1.local** и выберите **Свойства**.
18. На закладке **Общие** в поле **Динамическое обновление** выберите пункт **Да**.
19. Переключитесь на закладку **Передача зон** и установите переключатель в положение **Только на серверы, перечисленные на странице серверов имен**.
20. Нажмите **ОК** для завершения настройки.

Тема 5

Структура Active Directory

В этой теме:

Рассматриваются основные понятия и архитектура Active Directory. Объясняются различия между службой DNS и Active Directory.

Занятие 1: "Служба каталогов Active Directory".

Что такое служба каталогов?

Каталогом называется база данных, используемая для хранения сведений о необходимых объектах. Пример каталога - телефонный справочник, который содержащий данные о телефонных абонентах. В распределенных вычислительных системах или общедоступных компьютерных сетях, например в Internet, существует множество объектов - таких, как принтеры, серверы службы факсов, приложения, базы данных, пользователи. Пользователи должны уметь находить и использовать эти объекты, а администраторам необходимо управлять их использованием.

Служба каталогов отличается от каталога тем, что является одновременно базой данных и службой, которая обеспечивает доступ пользователей к данным.

Зачем нужна служба каталогов?

Служба каталогов - один из наиболее важных компонентов распределенной компьютерной системы. Пользователи и администраторы могут не знать точных имен интересующих объектов, а только один или несколько атрибутов этих объектов. Для получения списка объектов, обладающих этим атрибутом или набором атрибутов, они запрашивают каталог. Например: "Найти все принтеры с двусторонней печатью, расположенные в здании № 26". Служба каталогов позволяет пользователю найти любой объект в базе данных по заданному атрибуту.

Служба каталогов может решать следующие задачи:

- Обеспечивать уровень безопасности сети с помощью авторизации пользователя и контроля уровня его доступа к ресурсам.
- Обеспечивать поиск ресурсов в сети (компьютеров, принтеров и общих папок).
- Выполнять репликацию каталога, чтобы обеспечить доступ большему числу пользователей и повысить защищенность сети от сбоев.
- Разбивать каталог на несколько разделов, чтобы увеличить общую отказоустойчивость каталога и уменьшить объем репликации для каждого раздела.

Служба каталогов - это инструмент не только администратора, но и конечного пользователя. По мере роста числа объектов в сети повышается значение службы каталогов. Служба каталогов - это та ось, вокруг которой вращается вся информационная система организации.

Что такое Active Directory?

Active Directory - это служба каталогов, входящая в операционную систему Windows 2000 Server. В Active Directory хранятся записи для конкретных физических ресурсов (пользователей, компьютеров, принтеров ...). Сами эти записи называются объектами службы каталогов.

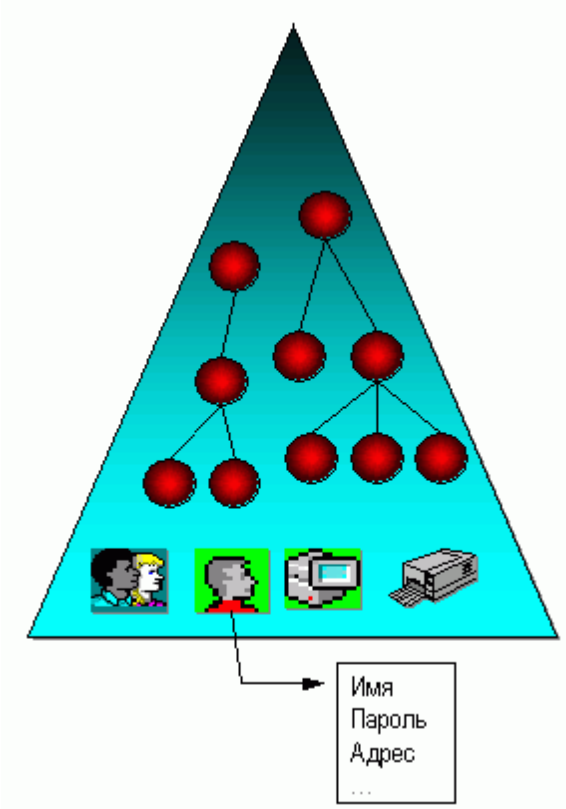
Создание централизованной базы данных, как и установка сетевой службы, обеспечивающей работу службы каталогов, происходят при установке Active Directory на сервер Windows 2000. После установки этот сервер выполняет роль контроллера домена, а остальные компьютеры (сервера и рабочие станции) необходимо ввести в состав домена. Для этих компьютеров и всех пользователей сети

должны быть созданы учетные записи в базе данных службы каталогов.

Занятие 2: "Основные понятия Active Directory".

Объект

Объект - это запись в базе даннных или набор атрибутов, представляющий нечто конкретное - пользователя, принтер, приложение. Атрибуты содержат данные, описывающие объект в каталоге. Так, атрибуты пользователя могут содержать его имя, фамилию и адрес электронной почты.



Контейнер

Контейнер подобен объекту в том, что у него есть атрибуты. Но в отличие от объекта, он не описывает нечто конкретное. Это "оболочка", объединяющая подмножество объектов и контейнеров. По аналогии с файловой системой контейнеры в домене можно сравнить с директориями и поддиректориями на диске. В Active Directory контейнеры используются для делегирования административных прав и назначения настроек через групповые политики.

Имя

Имена используются для различения объектов в Active Directory. Служба Active Directory допускает существование следующих типов имен.

Уникальное имя

Каждый объект в Active Directory имеет ***уникальное имя***. Это имя содержит указание на домен, в

котором находится объект, и полный путь в иерархической структуре контейнеров, который приводит к данному объекту. Типичным уникальным именем является имя

/DC=Company/DC=Ru/CN=Users/CN=Vasily Pupkin

Это имя обозначает объект типа "пользователь" с именем "Vasily Pupkin", находящийся в домене Company.Ru

Относительное имя

Относительное уникальное имя объекта - это та часть уникального имени, которая обозначает объект. Оно должно быть уникальным только в пределах родительского контейнера, что обеспечивает глобальную уникальность объектов Active Directory. В приведенном выше примере относительным именем объекта "Vasily Pupkin" является имя CN=Vasily Pupkin. Относительным именем родительского объекта является имя CN=Users.

Имя для входа в домен.

Каждый пользователь для входа в домен должен иметь ***имя для входа*** (logon name). Оно является атрибутом учетной записи (объекта для этого пользователя) и должно быть уникальным в пределах домена.

Домены

Домен - это централизованно управляемая система, хранящая информацию о сетевых ресурсах и пользователях. Домен является основной единицей администрирования и отдельной областью безопасности в сети Windows NT или Windows 2000. Каждый домен имеет свою отдельную группу администраторов домена и свои настройки безопасности. При управлении объектами администратор обычно работает только с базой данных в пределах одного домена. С физической точки зрения один домен может включать в себя компьютеры, расположенные в разных местах.

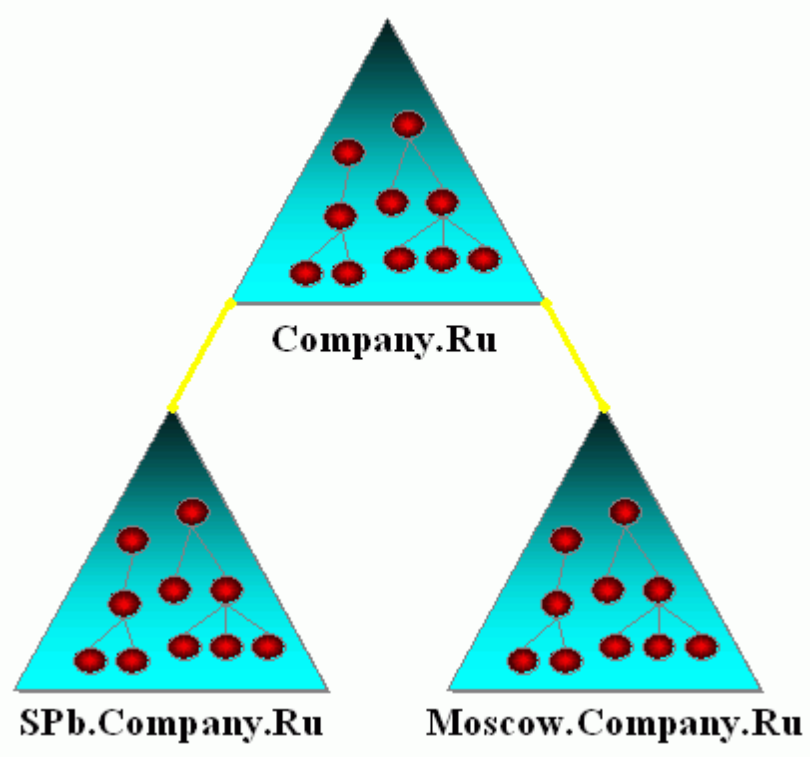
Служба каталогов Active Directory может состоять из одного или нескольких доменов. Сразу после установки первого контроллера домена Active Directory представлена только одним доменом, но всегда можно создать новые домены в той же Active Directory. Все домены в пределах одного **леса** Active Directory связаны **доверительными отношениями**, пользуются одной **схемой** (описанием всех возможных для этой базы данных объектов и их атрибутов), пользуются одним **глобальным каталогом** (общий индекс баз данных в каждом домене - используется при поисках по всему лесу).

Дерево доменов

Термин ***дерево*** используется для описания иерархии объектов и контейнеров. Вершины дерева обычно являются объектами. Узлы дерева (точки, где дерево ветвится) являются контейнерами. Дерево показывает связь между объектами или путь от одного объекта к другому.

Дерево доменов состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют *непрерывное пространство имен*. Домены в дереве связаны между собой доверительными отношениями. В лес Active Directory может входить одно или несколько деревьев.

Дерево графически можно представить через пространство доменных имен.

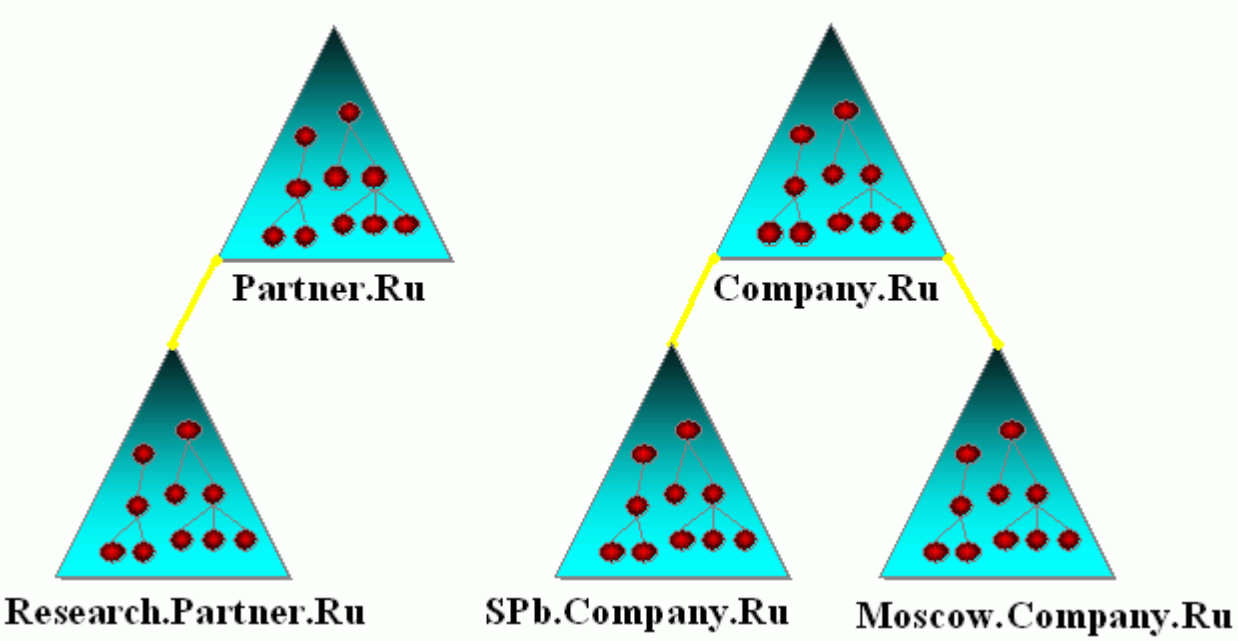


Уникальное имя объекта можно определить, двигаясь вверх по доменному дереву, начиная с объекта. Такой метод удобен при объединении объектов в логическую иерархическую структуру. Главное достоинство непрерывного пространства имен состоит в том, что глубокий поиск, проводимый от корня дерева, позволяет просмотреть все иерархические уровни пространства имен.

Лес

Лесом называется одно или несколько деревьев, которые **не образуют непрерывного пространства имен**. Все деревья одного леса имеют общую логическую структуру (схему), конфигурацию и глобальный каталог, и поддерживают друг с другом транзитные доверительные отношения, автоматически устанавливаемые на основе протокола Kerberos.

Корневой домен леса - первый домен, созданный в данной Active Directory. Только на нем существует группа ***Администраторы предприятия***, имеющая право на любые операции с Active Directory - например, добавление новых доменов.



Занятие 3: "Интеграция Active Directory со службой DNS"

Общие сведения об интеграции с DNS

Хотя Active Directory интегрируется с DNS и они имеют общую структуру пространства имен, нужно понимать разницу между ними.

- DNS является службой разрешения имен.

  Клиенты DNS посылают запросы на разрешение имен DNS на свой сервер DNS. Сервер DNS получает эти запросы и разрешает их с помощью локальных файлов или связывается с другим сервером DNS для разрешения имен. Для работы DNS не требуется Active Directory.
- Active Directory является службой каталога.

  Active Directory предоставляет хранилище данных и службы для предоставления данных пользователям и приложениям. Клиенты Active Directory посылают запросы на серверы с использованием протокола LDAP (Lightweight Directory Access Protocol). ***Для поиска сервера клиенты Active Directory посылают запросы на DNS.*** Поэтому для функционирования Active Directory требуется DNS.

Active Directory использует DNS в качестве службы адресации для разрешения доменов, сайтов и имен служб Active Directory в IP-адреса.

Для входа в домен Active Directory клиент сначала должен обнаружить контроллер для своего домена Active Directory. Для обнаружения контроллера определенного домена клиент Active Directory отправляет запрос на разрешение имени DNS на соответствующий сервер (серверы). Запрос имеет следующие характеристики.

- Тип записи: запись ресурса SRV
- Имя запроса: _ldap._tcp.*имя_домена*

Например, для входа в домен microinform.ru, клиент Active Directory отправляет запрос типа SRV на разрешение имени DNS _ldap._tcp.microinform.ru.

Ответ от DNS-сервера содержит DNS-имена контроллеров домена и соответствующие им IP-адреса. Используя список IP-адресов контроллеров домена, клиент пытается подключиться к каждому из них них по очереди для проверки работоспособности контроллеров домена. Первый контроллер домена, от которого получен ответ, используется для входа в сеть.

Требования к серверам DNS для Active Directory

Для корректного функционирования Active Directory серверы DNS должны поддерживать записи ресурсов типа SRV. Записи ресурсов типа SRV связывают имя службы с именем сервера, предоставляющего данную службу. Клиенты и контроллеры домена Active Directory используют записи SRV для определения IP-адресов контроллеров домена. Хотя это не является необходимым требованием для работы Active Directory, рекомендуется, чтобы серверы DNS поддерживали динамическое обновление записей в DNS.

Служба DNS в Windows 2000 поддерживает записи SRV и динамические обновления. Если используется сервер DNS, отличный от Windows 2000, следует проверить, поддерживает ли он, как минимум, записи ресурсов типа SRV. Если он не поддерживает данный тип записи, то требуется обновить сервер до соответствующей версии. Например, службу DNS в Windows NT Server 4.0 необходимо обновить до пакета обновления Service Pack 4 или более поздней версии для поддержки записей SRV.

Занятие 4: "Роли хозяев операций"

Active Directory поддерживает репликацию хранилища данных каталога между всеми контроллерами домена. Однако, некоторые изменения можно выполнять только на одном контроллере домена. Его называют *хозяином операции*, и только он принимает запросы на такие изменения. Роль хозяина операций может быть передана другим контроллерам в составе домена или леса.

Лес Active Directory содержит пять ролей хозяина операций, назначаемых одному или нескольким контроллерам домена. Некоторые роли должны быть в составе каждого леса. Остальные роли должны быть в каждом домене леса.

По умолчанию все пять ролей выполняет первый установленный в лес контроллер домена. Если планируется удалить его из сети, нужно передать все его пять ролей любому другому контроллеру в сети. При выходе из строя первого установленного контроллера (или если роли забыли передать до его удаления) можно присвоить эти роли. Как выполнить эти операции, описано в [занятии 5 темы 6 "Перемещения ролей хозяев операций"]

Роли хозяина операций на уровне всего леса

Каждый лес Active Directory должен содержать следующие роли.

- Хозяин схемы
- Хозяин именования домена

Данные роли должны быть уникальными в пределах леса. Это означает, что в пределах всего леса может быть только один хозяин схемы и один хозяин именования домена.

Хозяин схемы

Хозяин схемы управляет всеми обновлениями и изменениями схемы. Для обновления схемы леса необходимо иметь доступ к хозяину схемы. В любой момент времени может быть только один хозяин схемы в составе всего леса.

Хозяин именования домена

Контроллер домена, выполняющий роль хозяина именования домена, управляет операциями добавления или удаления доменов в составе леса. В любой момент времени может быть только один хозяин именования домена в составе всего леса.

Роли хозяина операций на уровне всего домена

Каждый домен Active Directory должен содержать следующие роли.

- Хозяин относительных идентификаторов
- Эмулятор основного контроллера домена
- Хозяин инфраструктуры

Эти роли должны быть уникальными в пределах каждого домена. Это означает, что в каждом домене в

составе леса может быть только один хозяин относительных идентификаторов, один эмулятор основного контроллера домена и один хозяин инфраструктуры.

Хозяин относительных идентификаторов

Хозяин относительных идентификаторов назначает ряд относительных идентификаторов каждому контроллеру в своем домене. В любой момент времени в каждом домене леса может быть только один контроллер домена, выполняющий роль хозяина относительных идентификаторов.

Каждый раз при создании объекта пользователя, группы или компьютера, контроллер домена назначает данному объекту уникальный код безопасности. Код безопасности состоит из кода безопасности домена (который одинаков для всех кодов безопасности, созданных в этом домене) и относительного кода безопасности, уникального для каждого кода безопасности, созданного в домене.

Эмулятор основного контролера домена

Если в домене есть компьютеры с операционными системами Windows 95/98/NT 4.0 без установленного клиентского программного обеспечения для Active Directory или резервные контроллеры домена Windows NT, эмулятор основного контроллера домена работает как основной контроллер домена Windows NT. Он обрабатывает изменения паролей от клиентов и реплицирует обновления на резервные контроллеры домена. В любой момент времени в каждом домене может быть только один контроллер домена, выполняющий роль эмулятора основного контроллера домена.

При работе домена Windows 2000 в основном режиме, эмулятор основного контроллера получает копию изменений пароля, выполненных другими контроллерами в данном домене. При изменении пароля репликация этих изменений на каждый контроллер домена занимает некоторое время. Если при входе в сеть проверка подлинности на одном контроллере домена заканчивается неудачно из-за ввода неверного пароля, прежде чем отказать в доступе, он пересылает запрос на проверку подлинности на эмулятор основного контроллера домена.

Хозяин инфраструктуры

Хозяин инфраструктуры отвечает за обновление ссылок "группа-пользователь" при переименовании или изменении членов группы. В любой момент времени в каждом домене может быть только один контроллер домена, выполняющий роль хозяина инфраструктуры.

При переименовании или перемещении члена группы (и размещении данного члена в другом домене, отличном от домена этой группы) он может временно не отображаться в группе. Хозяин инфраструктуры домена, содержащего данную группу, отвечает за обновление группы и обладает сведениями об имени и расположении данного члена. Хозяин инфраструктуры распространяет обновленные сведения с помощью репликации с несколькими хозяевами.

В период между переименованием члена группы и обновлением этой группы безопасность системы не подвергается риску. Только администратор, просматривающий участие в отдельной группе, может заметить временное несоответствие.

Тема 6

Администрирование Active Directory

В этой теме:

Рассматривается администрирование Active Directory с помощью инструмента "Active Directory - пользователи и компьютеры". Даются знания и практические навыки по управлению учетными записями пользователей, групп и компьютеров. Обсуждаются вопросы настройки политик безопасности. Описываются способы перемещения ролей хозяев операций.

Занятие 1: "Управление учетными записями пользователей"

Учетные записи пользователей Active Directory

Учетная запись Active Directory позволяет пользователю входить на компьютеры и в домен с использованием учетной записи. Каждый пользователь, входящий в сеть, должен иметь собственную учетную запись и пароль.

Windows 2000 предоставляет стандартные учетные записи пользователей Active Directory, которые могут использоваться для входа в домен. Существуют две стандартные учетные записи:

- Учетная запись администратора.
- Учетная запись гостя.

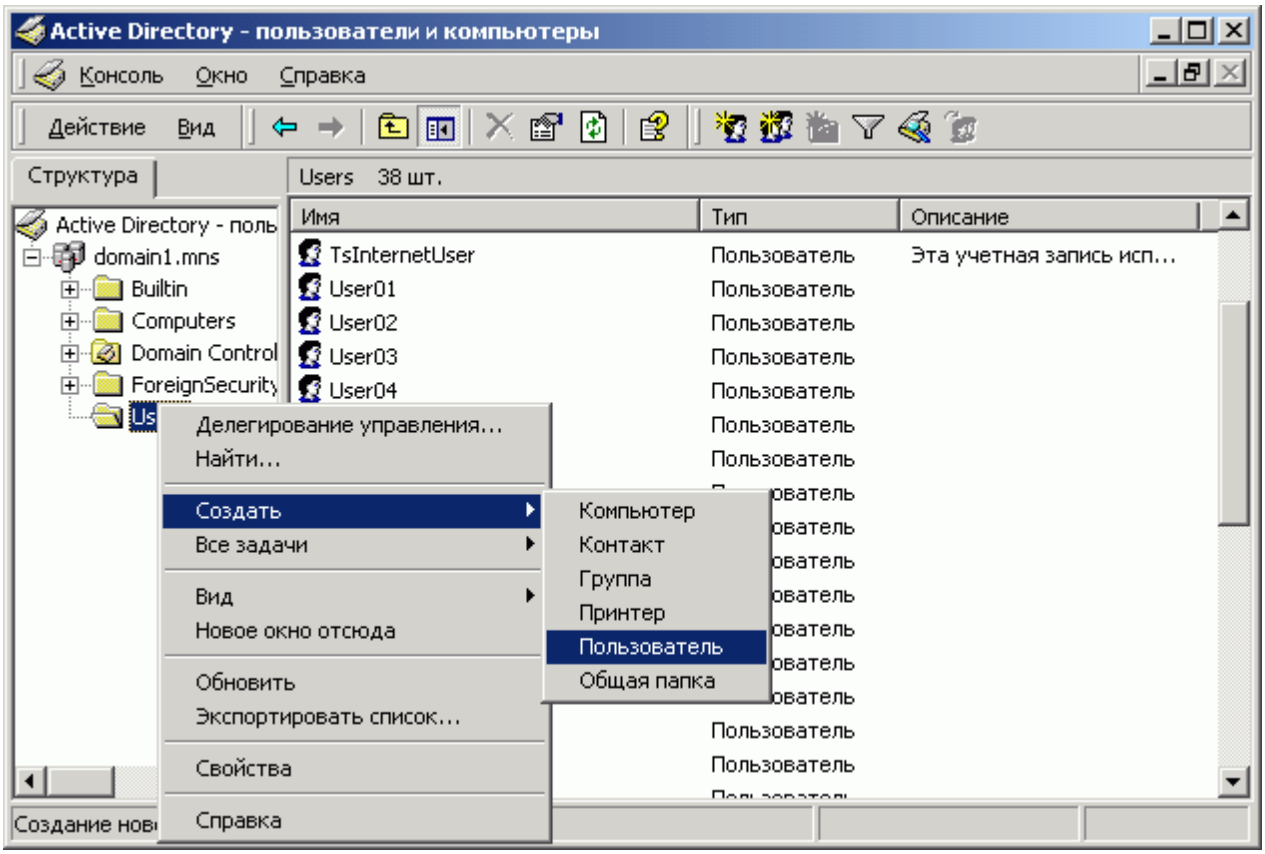
Стандартные учетные записи создаются по умолчанию и предназначены для входа на контроллер домена и доступа к его ресурсам. Они используются в основном для начального входа в систему и настройки домена. Каждая стандартная учетная запись имеет разную комбинацию прав и разрешений. Учетная запись администратора имеет самые большие права и разрешения, а учетная запись гостя - ограниченные права и разрешения, кроме того, изначально по умолчанию она отключена.

Стандартные учетные записи могут использоваться любым пользователем или службой для входа в сеть, но для обеспечения безопасности следует создавать отдельные учетные записи для каждого пользователя, входящего в сеть, с помощью инструмента "Active Directory - пользователи и компьютеры". Каждая учетная запись пользователя (включая учетные записи администратора и гостя) может быть добавлена в группу Windows 2000 для управления правами и разрешениями, назначенными этой учетной записи. Использование учетных записей и групп позволяет проверить подлинность входящего в сеть пользователя и возможность предоставления доступа к разрешенным ему ресурсам.

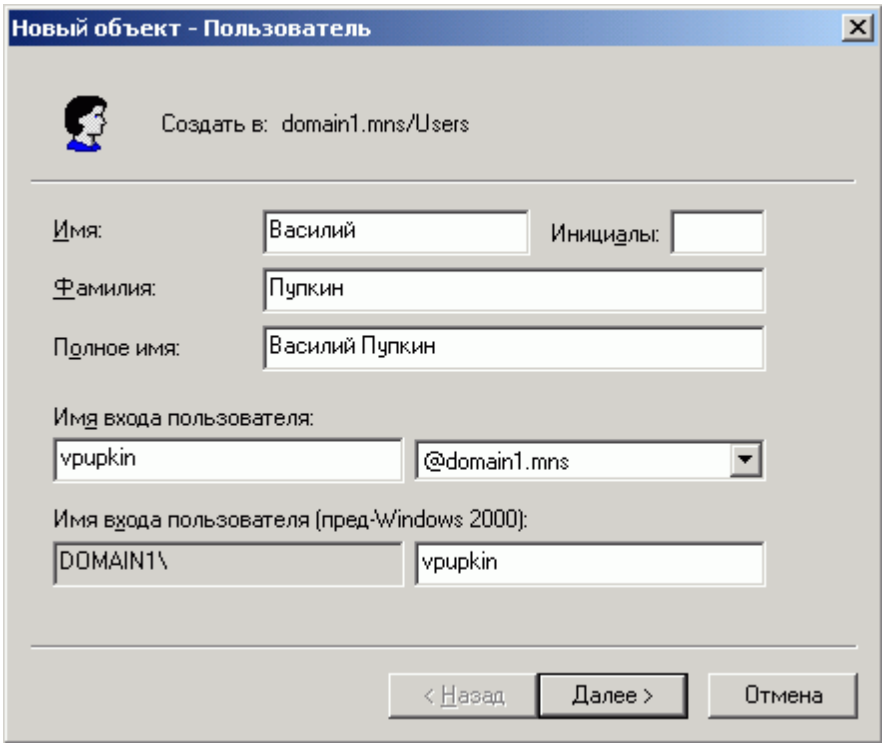
Чтобы использовать инструмент "Active Directory - пользователи и компьютеры", в **панели управления** последовательно выберите **Администрирование**, **Active Directory - пользователи и компьютеры**.

Создание учетной записи пользователя

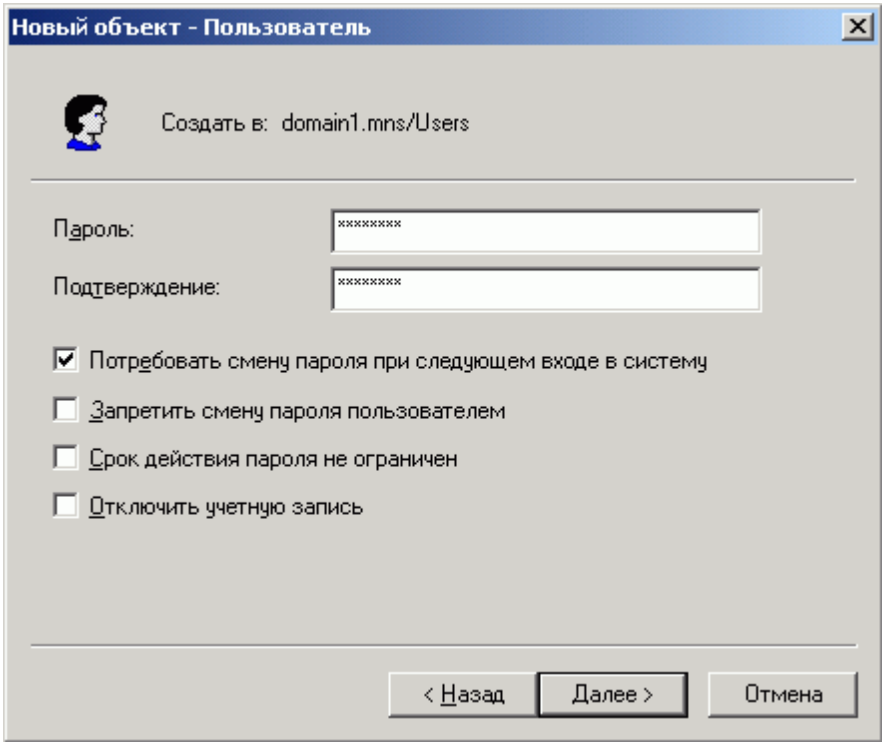
1. Откройте инструмент "Active Directory — пользователи и компьютеры".
2. В дереве консоли дважды щелкните узел домена.
3. На правой панели щелкните правой кнопкой мыши организационное подразделение (например, стандартный контейнер "Users"), в которое необходимо добавить пользователя, выберите **Создать**, **Пользователь**.



4. В поля **Имя**, **Инициалы** и **Фамилия** введите соответствующие данные для пользователя.
5. Измените сведения в поле **Полное имя**, если необходимо, чтобы в списках Active Directory учетная запись отображалась по-другому.
6. В поле **Имя входа пользователя** введите имя, под которым пользователь будет входить в домен.
7. Если пользователь будет входить на компьютеры под управлением Windows NT, Windows 98 или Windows 95, под разными именами, то следует указать другое имя в поле **Имя входа пользователя (пред-Windows 2000)**.



8. В полях **Пароль** и **Подтверждение** введите пароль пользователя.



9. Установите флажок **Потребовать смену пароля при следующем входе в систему**, чтобы только пользователь знал свой пароль и самостоятельно менял его. Иначе предполагается, что работой по установке паролей и их изменению занимается администратор домена.

После создания учетной записи пользователя измените ее свойства для ввода дополнительных сведений. Для добавления пользователя также можно скопировать ранее созданную учетную запись.

Удаление учетной записи пользователя

Для удаления учетной записи пользователя в инструменте "Active Directory — пользователи и компьютеры" щелкните учетную запись правой кнопкой мыши и выберите **Удалить**.

Внимание! Новая учетная запись пользователя с тем же именем, что и ранее удаленная, не получает разрешения и участие в группах ранее удаленной учетной записи, так как дескриптор безопасности для каждой учетной записи уникален. Для создания копии удаленной учетной записи все разрешения и участие в группах необходимо восстановить вручную. Поэтому вместо удаления рекомендуется отключать учетные записи.

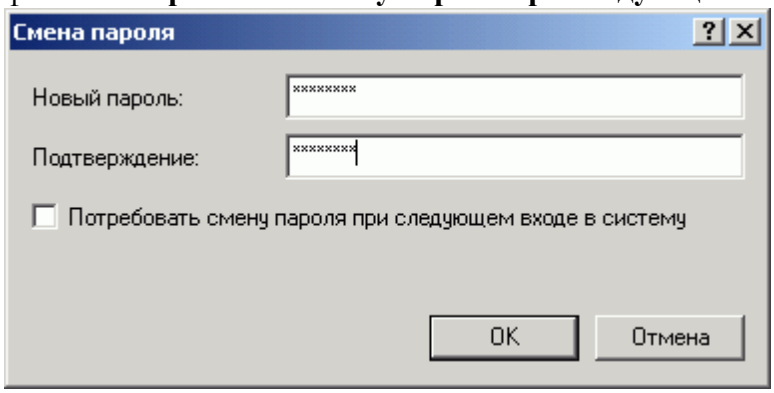
Отключение учетной записи пользователя

Для предотвращения входа в сеть определенных пользователей их учетные записи вместо полного удаления могут быть отключены. Для отключения учетной записи пользователя в инструменте "Active Directory — пользователи и компьютеры" щелкните учетную запись правой кнопкой мыши и выберите **Отключить учетную запись**.

Изменение пароля для учетной записи пользователя

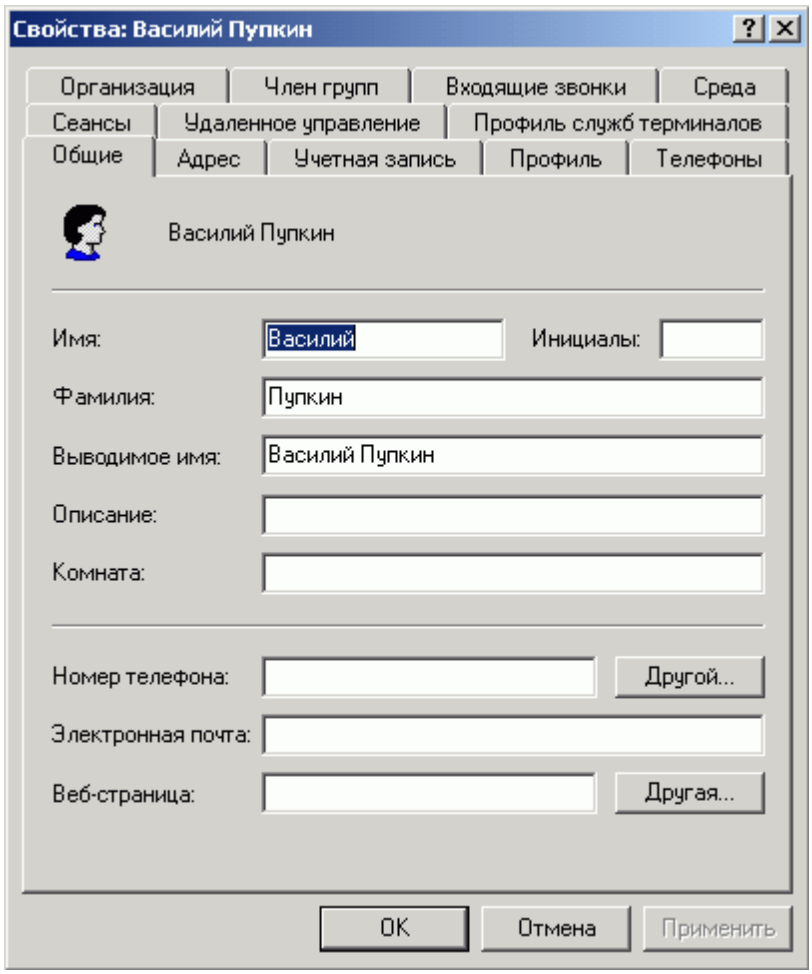
Для изменения пароля учетной записи пользователя щелкните правой кнопкой мыши учетную запись и выберите **Смена пароля**. Введите новый пароль и подтверждение. **Внимание!** Для смены пароля знать старый пароль не требуется.

Если политика организации допускает самостоятельную установку пароля пользователем, установите флажок **Потребовать смену пароля при следующем входе в систему**.



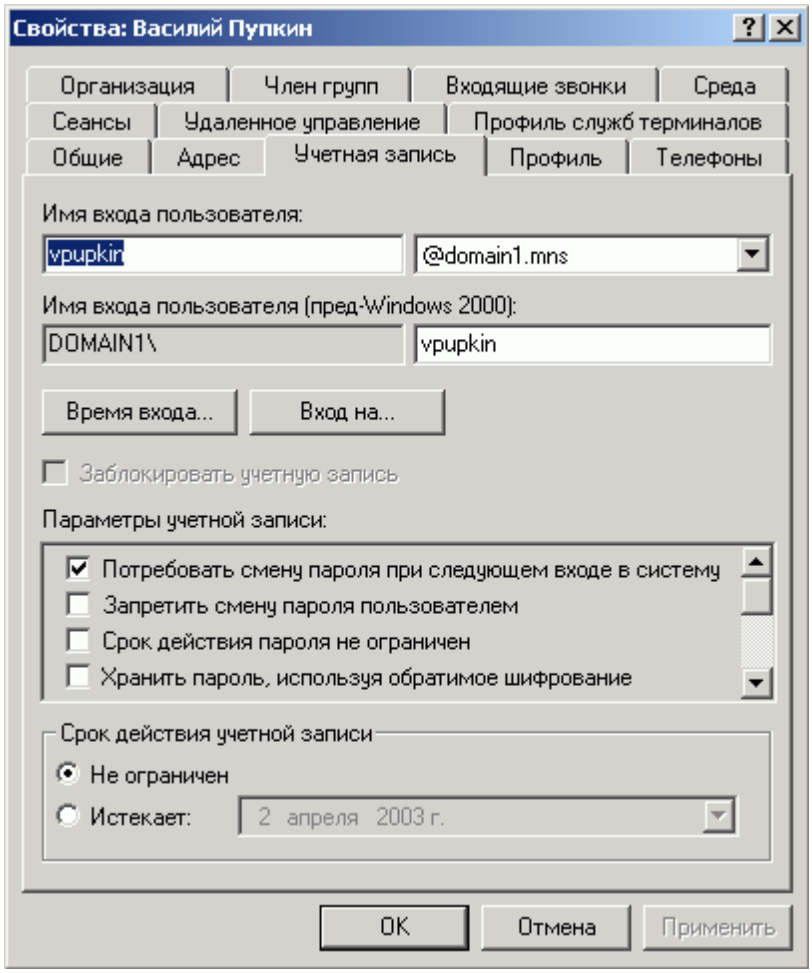
Изменение свойств учетной записи пользователя

Кроме обязательных параметров при создании учетной записи стоит заполнить некоторые из необязательных полей. На закладке **Общие** можно изменить имя и фамилию пользователя, если при создании учетной записи они введены неправильно, а также можно добавить номер телефона, комнаты, адрес электронной почты данного пользователя. Заполнение необязательных полей позволит пользователям применять Active Directory как справочник, в котором можно найти дополнительную информацию о коллегах.



Еще одна закладка в свойствах учетной записи пользователя - **Учетная запись**. Здесь можно изменить имя учетной записи пользователя, под которой он входит в сеть, установить ограничения по времени

работы или используемым рабочим станциям, а также задать дополнительные настройки по безопасности - **Потребовать смену пароля при следующем входе в систему**, **Запретить смену пароля пользователем**, **Срок действия пароля не ограничен** и т.д.



Упражнение 6.A: "Создание и изменение учетных записей пользователей домена"

Краткое описание

В этом упражнении Вы научитесь создавать учетные записи пользователей в домене.

Предварительные требования к выполнению упражнения

Вы должны самостоятельно установить Windows 2000 Server и Active Directory, чтобы выполнить эту и последующие работы в теме 6. Предполагается, что навыки установки сервера и Active Directory Вы получили в результате прослушивания очных курсов.

Порядок выполнения упражнения

1. Войдите в домен под учетной записью пользователя, имеющего права администратора домена.
2. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **Active Directory - пользователи и компьютеры**
3. Правой кнопкой щелкните на папке **Users** и выберите **Создать**, **Пользователь**.
4. В поле **Имя** введите ***Василий***, а в поле **Фамилия** - ***Пупкин***. В поле **Имя входа пользователя** введите ***vpupkin*** и нажмите **Далее**
5. Введите в поле **Пароль** и **Подтверждение пароля** ***userpassword*** и нажмите **Далее**. Нажмите **Готово** для создания пользователя.
6. Правой кнопкой щелкните на папке **Users** и выберите **Создать**, **Пользователь**.
7. В поле **Имя** введите ***Александр***, а в поле **Фамилия** - ***Администов***. В поле **Имя входа пользователя** введите ***admin*** и нажмите **Далее**
8. Введите в поле **Пароль** и **Подтверждение пароля** ***adminpassword*** и нажмите **Далее**. Нажмите **Готово** для создания пользователя.
9. Нажмите **ОК**, чтобы сохранить изменения.
10. Правой кнопкой щелкните на учетной записи **Василий Пупкин** и нажмите **Свойства**.
11. На закладке **Общие** в поле ***Комната*** введите ***203***, в поле ***Телефон*** введите ***42-03*** а в поле **Электронная почта** - ***vasyapupkin@hotmail.ru***
12. На закладке **Учетная запись** щелкните на **Время входа...** и разрешите для этой учетной записи работу только с 8 часов утра до 19 часов вечера.
13. Последовательно выберите **Пуск Найти**, **Людей...**
14. Выберите **Место поиска** - ***Active Directory*** и в поле **Имя** введите ***Василий***.
15. Нажмите **Найти**. Удостоверьтесь, что была найдена учетная запись пользователя **Василий Пупкин**.

Занятие 2: "Управление учетными записями групп"

Типы и области действия групп

Типы групп

В Active Directory существует два типа групп.

- Группы безопасности
- Группы распространения

Группы безопасности используются в избирательных таблицах управления доступом (DACL), определяющих разрешения для ресурсов и объектов.

Группы распространения не используются для безопасности. Они не могут быть включены в DACL. Группы распространения используются только приложениями электронной почты (например, Exchange) для отправки сообщений электронной почты группам пользователей.

Области действия групп

Каждая группа безопасности и распространения имеет область действия, определяющую диапазон в дереве доменов или лесе, в котором применяется группа:

- Группы с глобальной областью действия (или глобальные группы) могут иметь в качестве членов группы и учетные записи только из домена, в котором определена данная группа. Ей могут быть предоставлены разрешения в любом домене леса. Глобальные группы используются, как списки пользователей из данного домена, которым надо предоставить доступ к ресурсу. Глобальные группы включаются в локальные группы домена для получения разрешения на ресурсы.
- Группы с локальной доменной областью действия (или локальные группы домена) могут иметь в качестве членов группы и учетные записи из домена Windows 2000 или Windows NT и использоваться для предоставления разрешений только в пределах домена. Локальным группам домена предоставляются разрешения на доступ к ресурсу, и уже в них включаются глобальные группы (списки пользователей, которым необходим доступ).

Встроенные локальные и глобальные группы

Встроенные группы устанавливаются в папки Builtin и Users консоли «Active Directory — пользователи и компьютеры» при установке контроллера домена. Это - группы безопасности и содержат общие наборы прав и разрешений, которые могут быть использованы для предоставления некоторых ролей, прав и разрешений учетным записям и группам, помещаемым в данные группы.

Локальные группы по умолчанию расположены в папке Builtin, глобальные группы расположены в папке Users. Можно перемещать встроенные и стандартные группы в папки других групп или подразделений домена, но не в другие домены.

Встроенные локальные группы

- **Операторы учета** - имеют права на все операции с учетными записями в домене, а также право локального входа на контроллеры домена.
- **Администраторы** - имеют все права в домене
- **Операторы архива** - имеют права архивировать и восстанавливать файлы на контроллерах домена, независимо от всех разрешений, которыми защищены эти файлы. Также они имеют право локального входа на контроллеры домена.
- **Гости** - имеют права доступа по сети к контроллеру домена с ограниченными возможностями (для случайных или разовых пользователей).
- **Операторы печати** - имеют права управлять всеми принтерами и документами, печатающимися на них.
- **Операторы сервера** - имеют права на все операции с сервером, кроме управления учетными записями в домене, а также право локального входа на контроллеры домена.
- **Пользователи** - имеют права доступа по сети к контроллеру домена. В эту группу входят все учетные записи, кроме гостей.

Данные встроенные локальные группы имеют область действия в пределах домена и в основном используются для назначения стандартного набора прав пользователям, которым необходимы некоторые административные права в домене.

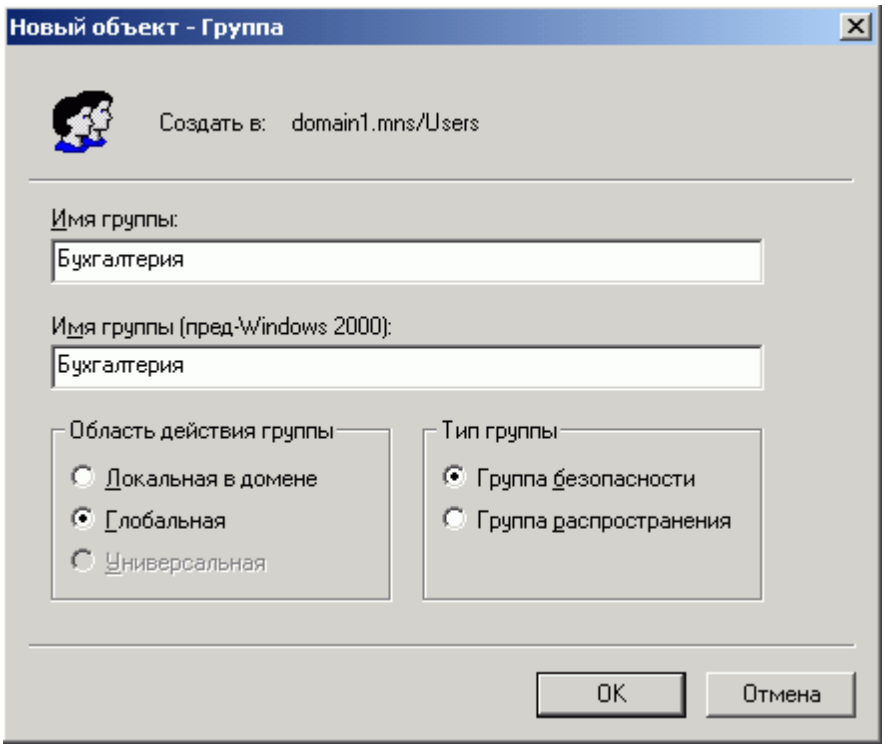
Встроенные глобальные группы

- **Администраторы домена** - список всех администраторов в домене. По умолчанию группа «Администраторы домена» данного домена входит в состав группы «Администраторы» в этом же домене. Windows 2000 не помещает автоматически учетные записи в эту группу, но если необходимо присвоить учетной записи широкие административные полномочия в домене, можно включить данную учетную запись в группу «Администраторы домена».
- **Гости домена** - список всех гостей в домене. По умолчанию группа «Гости домена» является членом группы «Гости» в этом же домене и автоматически включает в себя стандартную учетную запись домена «Гость».
- **Пользователи домена** - список всех пользователей в домене. По умолчанию любая учетная запись пользователя, созданная в домене, автоматически добавляется в группу «Пользователи домена», а группа «Пользователи домена» входит в состав группы «Пользователи» в этом же домене. Можно использовать группу «Пользователи домена» для обозначения всех учетных записей, созданных в домене.
- **Администраторы предприятия** - список администраторов, имеющих права на весь лес (то есть, все домены, входящие в него).
- **Администраторы схемы** - список администраторов, имеющих право внесения изменений в схему (структуру базы данных Active Directory).

Данные встроенные глобальные группы используются для объединения в группы различных видов учетных записей пользователей (обыкновенных пользователей, администраторов, гостей). Эти группы могут входить в состав групп с областью действия в пределах домена, в данном и других доменах.

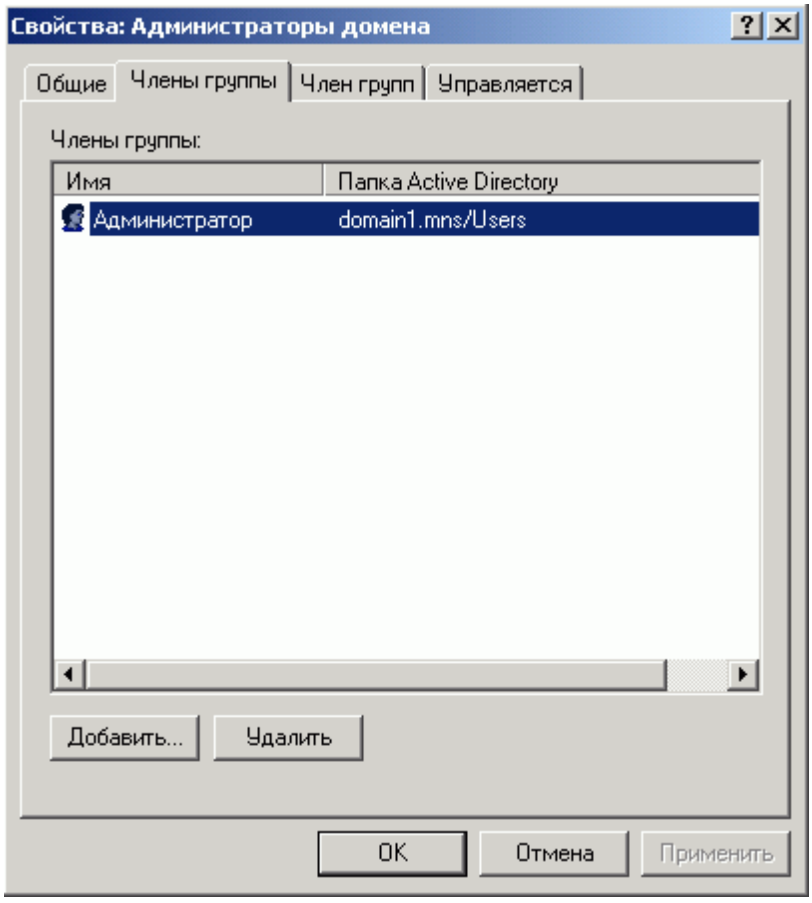
Создание группы

1. Откройте инструмент "Active Directory — пользователи и компьютеры".
2. В дереве консоли дважды щелкните узел домена.
3. Щелкните правой кнопкой папку, в которую необходимо добавить группу, выберите **Создать**, **Группа**.
4. Введите имя создаваемой группы. По умолчанию это имя также вводится как пред-Windows 2000 имя новой группы.
5. Выберите **Область действия группы** - локальная или глобальная и **Тип группы** - безопасности или распространения.



Изменение свойств группы

Основная закладка в свойствах группы - **Члены группы**. Здесь можно менять состав участников этой группы. Закладка **Член групп** показывает для глобальных групп, в какие локальные группы они включены.



Упражнение 6.Б: "Создание и изменение учетных записей групп в домене"

Краткое описание

В этом упражнении Вы научитесь создавать учетные записи локальных и глобальных групп в домене, и добавлять в них пользователей.

Предварительные требования к выполнению упражнения

Вы должны самостоятельно установить Windows 2000 Server и Active Directory, чтобы выполнить эту и последующие работы в теме 6. Предполагается, что навыки установки сервера и Active Directory Вы получили в результате прослушивания очных курсов. Кроме того, необходимо выполнить упражнение 6.А.

Порядок выполнения упражнения

1. Войдите в домен под учетной записью пользователя, имеющего права администратора домена.
2. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **Active Directory - пользователи и компьютеры**
3. Правой кнопкой щелкните на папке **Users** и выберите **Создать**, **Группа**.
4. В поле **Имя группы** введите ***Региональные администраторы***, выберите **Область действия группы** - ***глобальная***. Нажмите **ОК** для создания группы.
5. Правой кнопкой щелкните на учетной записи **Василий Пупкин** и нажмите **Добавить участников в группу...**.
6. Выберите группу **Региональные администраторы** и нажмите **ОК** для добавления пользователя, потом еще раз **ОК** для подтверждения операции.
7. Щелкните на контейнер **Builtin**, выберите группу **Операторы учета**. Щелкните на ней правой кнопкой, выберите **Свойства**.
8. На закладке **Члены групп** нажмите **Добавить...**, выберите группу **Региональные администраторы** и нажмите **ОК**. Нажмите **ОК**, чтобы сохранить изменения.

Занятие 3: "Управление учетными записями компьютеров"

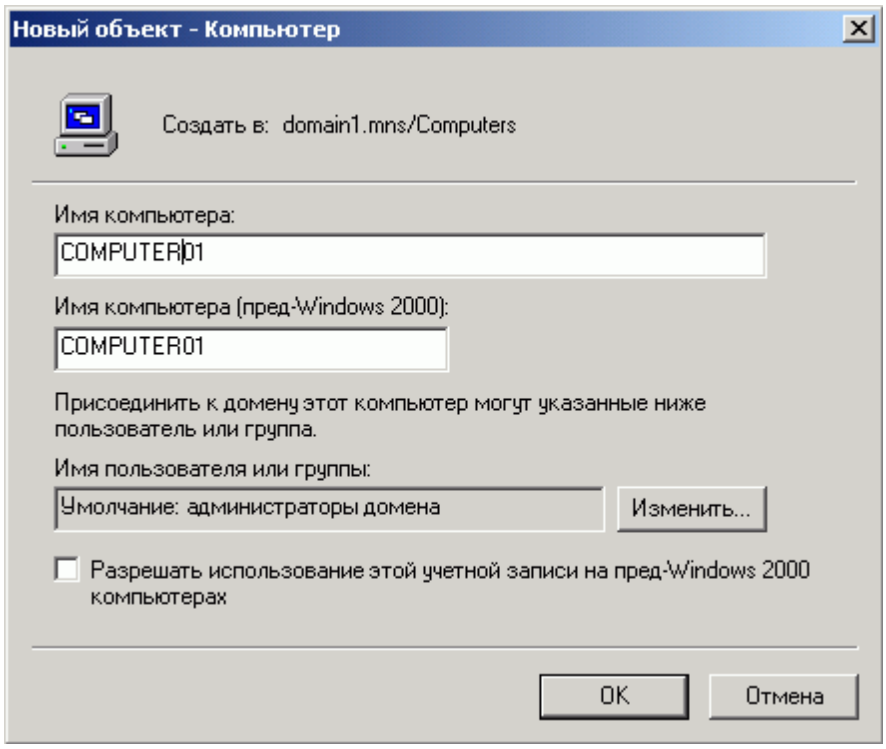
Каждый компьютер, работающий под управлением Windows XP, Windows 2000 или Windows NT, который присоединяется к домену, имеет учетную запись. Она, как и учетная запись пользователя, делает возможной проверку подлинности и аудит доступа компьютера к сети, а также доступ к ресурсам домена. Каждый подключенный к сети компьютер должен иметь собственную уникальную учетную запись. Эти записи создаются с помощью инструмента "Active Directory - пользователи и компьютеры".

Компьютеры под управлением Windows 98 и Windows 95 не имеют дополнительных функций безопасности, предоставляемых Windows 2000 и Windows NT, для них не создаются учетные записи компьютеров в доменах Windows 2000. Однако компьютеры под управлением Windows 98 и Windows 95 могут входить в сеть и работать в доменах Active Directory.

Создание учетной записи компьютера

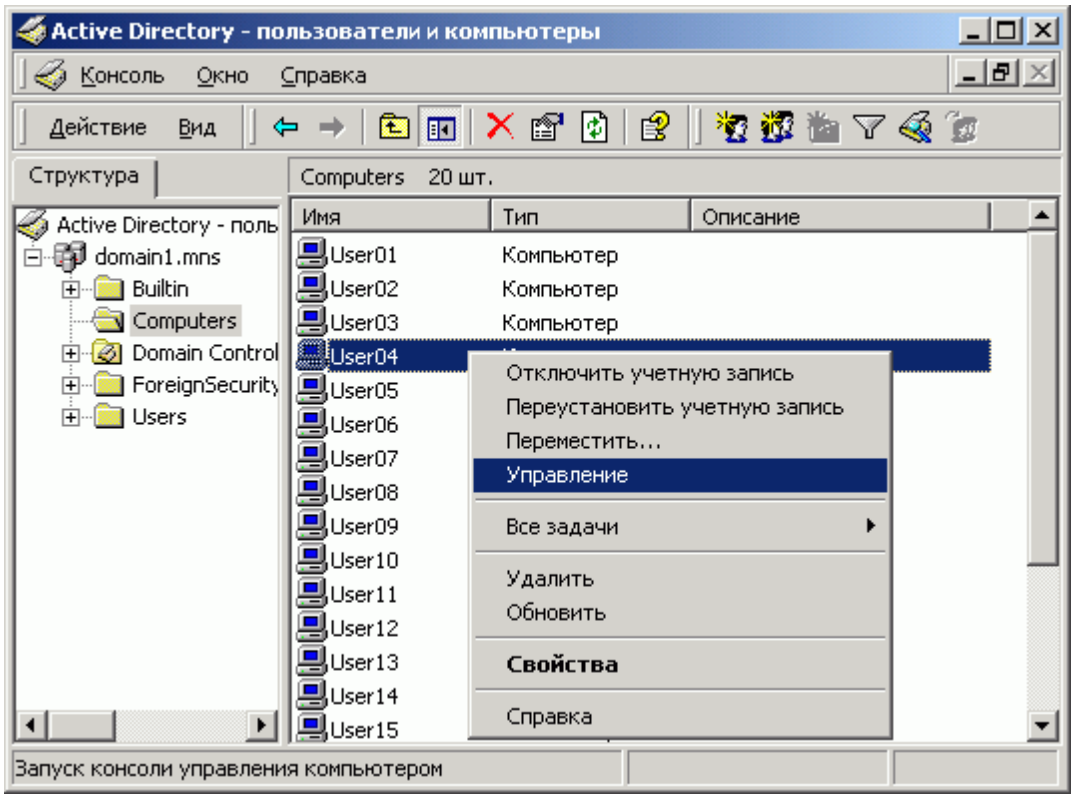
Учетная запись компьютера создается автоматически во время подсоединения компьютера к домену (только для Windows XP/2000/NT 4.0). Можно создать учетную запись компьютера и до подключения компьютера к домену, тогда для подключения компьютера пользователю будет достаточно иметь права локального администратора на этот компьютер, а не администратора домена, как в первом случае.

Чтобы создать учетную запись компьютера, запустите инструмент "Active Directory - пользователи и компьютеры", щелкните правой кнопкой мыши на организационное подразделение (рекомендуется стандартный контейнер "Computers"), где будет создана учетная запись, выберите **Создать**, **Компьютер** и введите имя компьютера (не более 15 символов). Кроме того, можно выбрать пользователей, обладающих правом подключения компьютера к данному домену. С помощью этой функции администратор может создать учетную запись компьютера и списки пользователей, обладающих ограниченными правами по установке компьютера и подключению его к домену.



Управление компьютером

Теперь, после создания учетной записи компьютера, можно осуществлять удаленное управление этим компьютером: проводить диагностику служб, работающих на этом компьютере, осуществлять просмотр событий и т.д. Для этого используется инструмент "Управление компьютером": щелкните учетную запись компьютера правой кнопкой мыши и выберите команду **Управление**.

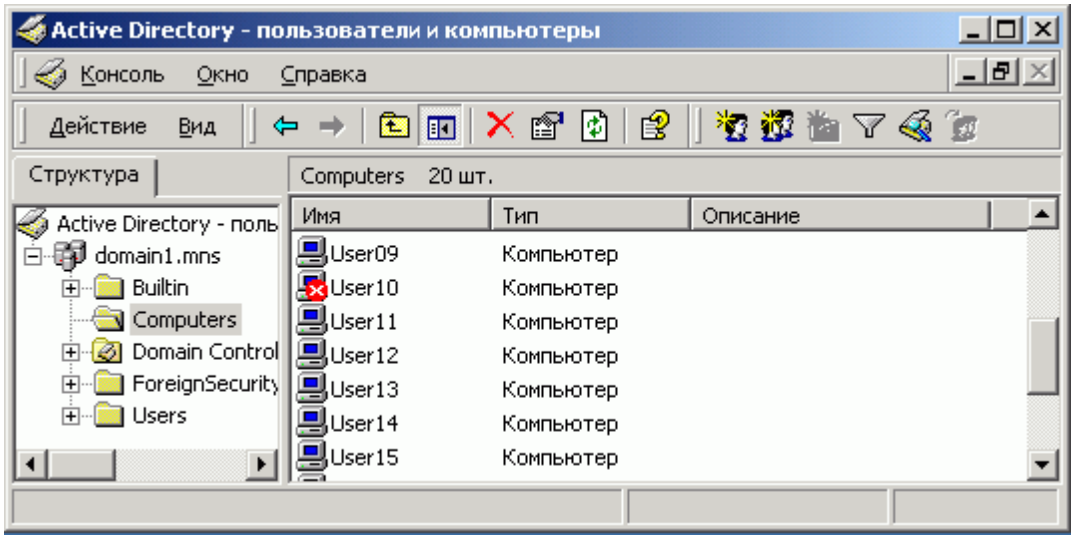


Отключение учетной записи компьютера

Компьютер, который больше не используется в домене, необходимо отключить. Эта операция прекращает его подключение к домену и он не сможет проходить проверку подлинности в домене,

пока учетная запись не будет включена.

Чтобы отключить учетную запись компьютера, запустите инструмент "Active Directory - пользователи и компьютеры", щелкните правой кнопкой мыши на компьютер и выберите **Отключить учетную запись**. Отключенный компьютер показывается в инструменте "Active Directory - пользователи и компьютеры" с красным кружком и белым крестом на нем:



Занятие 4: "Основы настройки политики безопасности"

Настройки безопасности определяют поведение системы, имеющее отношение к безопасности. Используя объекты групповой политики в Active Directory, администраторы могут централизованно настраивать уровни безопасности, необходимые для защиты системы предприятия.

При определении параметров для объектов групповой политики, содержащих несколько компьютеров, необходимо учитывать организационный и функциональный характер данного домена или подразделения. Например, уровень безопасности подразделения, включающего компьютеры отдела кадров, будут существенно отличаться от уровня безопасности подразделения компьютеров бухгалтерии.

Для домена Active Directory основные настройки политик безопасности выполняются на двух уровнях: политики учетных записей - для всего домена ("Политика безопасности домена"), права пользователей и дополнительные настройки определяются для контроллеров домена ("Политика безопасности контроллера домена").

Настройка политики безопасности на уровне всего домена

Для домена настройка политики безопасности выполняется с помощью инструмента "Политика безопасности домена". Основные настройки, которые необходимо понимать на этом уровне - это политика для паролей и политика блокировки учетных записей.

Политика для паролей

Обычно пароли - одно из слабых мест в системе безопасности компьютера. Очень важно использовать надежные пароли, поскольку программные средства и компьютеры, используемые для взлома паролей, продолжают улучшаться и становятся все более мощными.

Программное обеспечение для взлома паролей использует подбор вариантов по словарю или автоматический перебор всех возможных комбинаций символов. Имея достаточно времени, методом автоматического перебора можно взломать любой пароль. Однако для взлома надежного пароля требуются месяцы и годы.

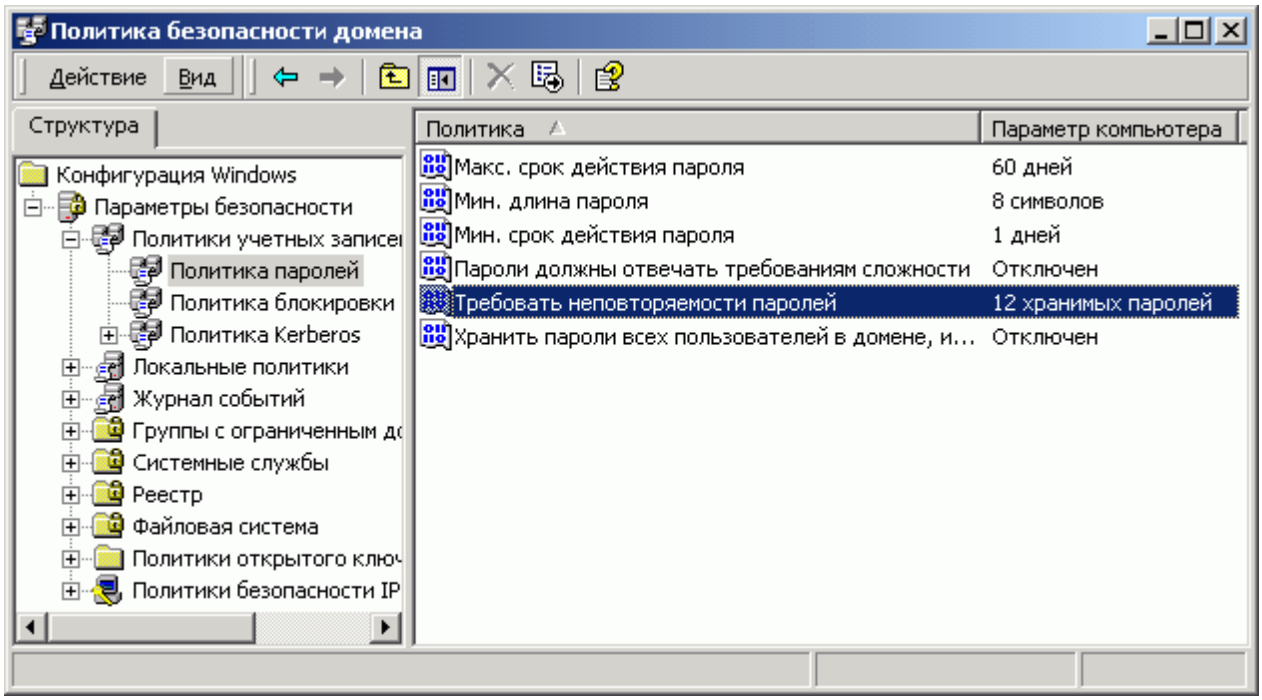
Высокий уровень безопасности компьютеров в домене предполагает использование надежных паролей для входа в сеть и учетной записи администратора в домене и на локальных компьютерах.

Рекомендуется устанавливать следующие требования к паролям:

- Длина пароля должна быть не менее восьми символов (параметр **Мин. длина пароля**).
- Пароль должен содержать символы каждой из трех следующих групп - буквы (прописные и строчные), цифры, прочие символы (параметр **Пароли должны отвечать требованиям сложности**). Бывает трудно приучить пользователей использовать сложные пароли, поэтому обычной практикой является не принуждение к таким паролям, а рекомендация к их использованию. Поэтому обычно параметр **Пароли должны отвечать требованиям сложности** оставляют в положении **Отключен**.
- Пароль должен существенно отличаться от предыдущих паролей. Можно хранить историю

паролей и с помощью параметра **Требовать неповторяемости паролей** контролировать ее. При включении этого параметра пользователь не сможет использовать свой предыдущий пароль второй раз.

- Пароль необходимо менять каждые 60-90 дней (параметр **Макс. срок действия пароля**).
- Кроме максимального срока действия, рекомендуется устанавливать параметр **Мин. срок действия пароля**. Это необходимо, чтобы пользователь не мог в один день сменить подряд несколько паролей и вернуться к старому.
- Пароль не должен содержать личного имени или имени пользователя, а также не являться распространенным словом или именем. Это не контролируется средствами Windows 2000, однако стоит довести это требование до пользователей в виде приказа или инструкции.



Политика блокировки учетных записей

Блокировка учетной записи позволяет задать определенное число попыток удаленного доступа с данной учетной записью, не проходящих проверку подлинности, после которого доступ пользователю с блокированной учетной записью будет запрещен. Злоумышленники могут пытаться получить доступ к сети путем перебора возможных паролей (т.н. словарная атака). Для этого "пользователь" посылает сотни и тысячи различных учетных данных, используя список паролей, основанных на общеупотребимых словах или фразах.

Если блокировка учетной записи включена, попытки доступа путем перебора известных слов будут пресекаться после определенного количества неудачных попыток. Сетевой администратор должен определить значения двух переменных, используемых при блокировке учетных записей.

1. Число неудачных попыток, после которого все дальнейшие попытки будут отклоняться - параметр **Пороговое значение блокировки**.

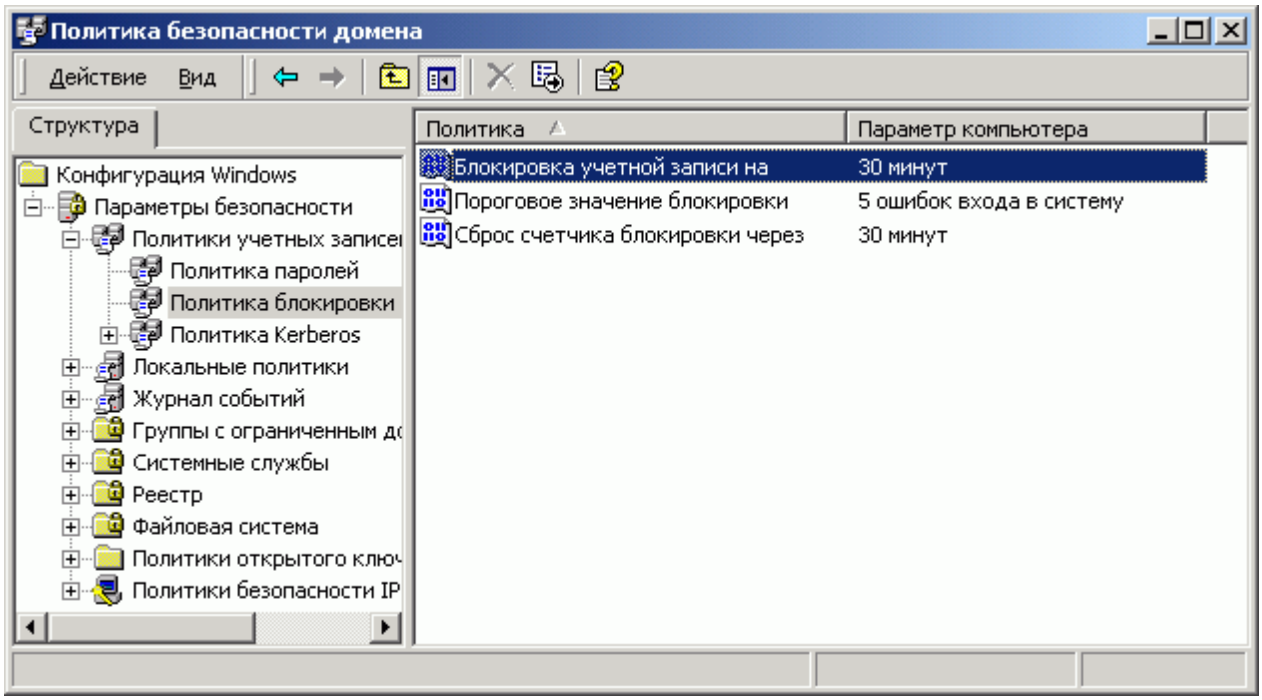
   После каждой неудачной попытки доступа увеличивается значение счетчика неудачных попыток учетной записи пользователя. Если значение счетчика неудачных попыток с данной учетной записью пользователя достигает заданного максимума, последующие попытки доступа будут отклоняться.

   Попытка доступа, успешно прошедшая проверку подлинности, сбрасывает счетчик неудачных попыток, если его значение меньше заданного максимума. Другими словами, счетчик неудачных попыток доступа после успешной попытки доступа начинает накапливать неудачные попытки заново.

2. Частоту сброса счетчика неудачных попыток определяет параметр **Сброс счетчика неудачных попыток**.

   Для того чтобы предотвратить длительную блокировку учетных записей, вызванную обычной невнимательностью пользователей при вводе паролей, необходимо периодически сбрасывать счетчик неудачных попыток.
3. Время блокировки учетных записей определяет параметр **Блокировка учетных записей на**.

   Этот параметр задается, чтобы блокировка автоматически снималась через указанный промежуток времени. Иначе администратор должен будет зайти в свойства учетной записи пользователя с помощью инструмента "Active Directory - пользователи и компьютеры" и снять флажок **Заблокировать учетную запись**.



Настройка политик безопасности на уровне контроллеров домена

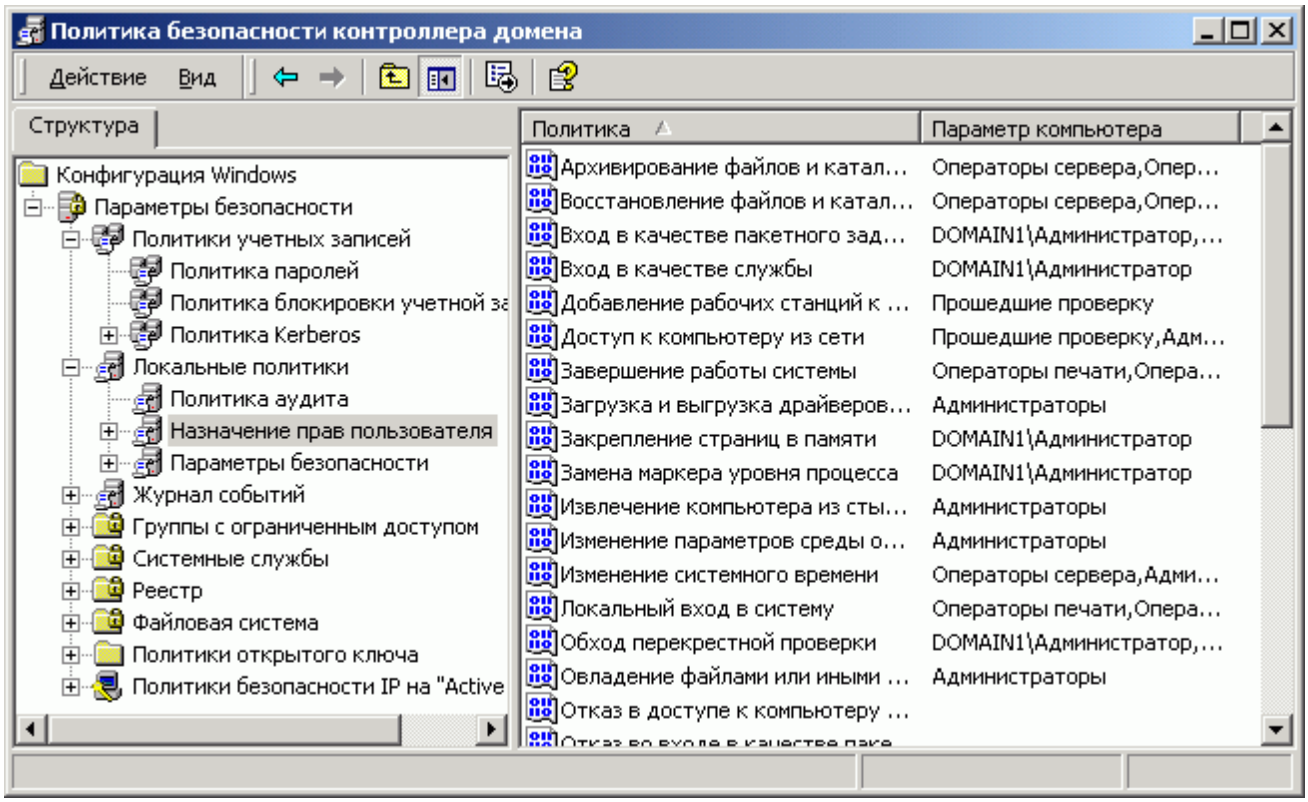
Для контроллеров домена настройка политики безопасности выполняется с помощью инструмента "Политика безопасности контроллера домена".

Ключевой момент при настройке безопасности на уровне контроллеров домена - правильно назначенные привилегии пользователей. Администраторы могут назначать привилегии учетным записям групп или отдельных пользователей. Эти привилегии позволяют пользователям выполнять конкретные действия, такие как интерактивный вход в систему или архивирование файлов и каталогов. Привилегии пользователей отличаются от разрешений тем, что применяются к учетным записям пользователей, а не к объектам. Основные привилегии перечислены и описаны в следующей таблице:

Привилегия	**Описание**

Архивирование файлов и каталогов	Эта привилегия позволяет пользователю избежать действия разрешений файлов и каталогов для архивирования системы. Эта привилегия равнозначна назначению следующих разрешений для всех файлов и папок во всем домене: «Обзор папок / Выполнение файлов», «Содержание папки / Чтение данных», «Чтение атрибутов», «Чтение дополнительных атрибутов» и «Чтение разрешений». Эту привилегию должна иметь только группа "Администраторы".
Изменение системного времени	Пользователь получает возможность устанавливать время на системных часах контроллеров домена. Эту привилегию должна иметь только группа "Администраторы".
Принудительное удаленное завершение	Пользователь получает возможность завершать работу контроллеров домена удаленно по сети. Эту привилегию должна иметь только группа "Администраторы".
Загрузка и выгрузка драйверов устройств	Пользователь получает возможность устанавливать и удалять драйверы самонастраиваемых устройств. Эта привилегия не влияет на драйверы устройств, не являющихся самонастраиваемыми, и эти драйверы могут быть только установлены. Поскольку драйверы устройств выполняются как доверенные (с более высоким приоритетом) программы, эта привилегия может быть неправильно использована для установки опасных программ, способных повредить систему, и предоставления этим программам доступа к ресурсам. Эту привилегию должна иметь только группа "Администраторы".
Восстановление файлов и каталогов	Пользователь получает возможность восстанавливать заархивированные файлы и каталоги, несмотря на их разрешения, а также назначать любого допустимого участника безопасности владельцем объекта. Эту привилегию должна иметь только группа "Администраторы".
Завершение работы системы	Пользователь получает возможность завершать работу операционной системы на локальном компьютере. Эту привилегию должна иметь только группа "Администраторы".
Овладение файлами или иными объектами	Пользователь получает возможность становиться владельцем любых объектов безопасности системы, включая объекты Active Directory, файлы и папки, принтеры, разделы реестра, процессы и потоки. Эту привилегию должна иметь только группа "Администраторы", иначе пользователям будет открыт доступ ко всем объектам, вне зависимости от разрешений.

Доступ к компьютеру из сети	Пользователю разрешен доступ при обращении к контроллеру домена по сети. По умолчанию доступ разрешен всем и менять этот параметр не рекомендуется.
Локальный вход в систему	Пользователю разрешен локальный вход на контроллер домена. Локальным входом считается вход с консоли сервера и вход через службу терминалов. По умолчанию он не разрешен обычным пользователям.



Упражнение 6.B: "Настройка политики безопасности для домена"

Краткое описание

В этом упражнении Вы научитесь настраивать политику для паролей и политику блокировки учетных записей на домен

Предварительные требования к выполнению упражнения

Вы должны самостоятельно установить Windows 2000 Server и Active Directory, чтобы выполнить эту работу. Предполагается, что навыки установки сервера и Active Directory Вы получили в результате прослушивания очных курсов. Кроме того, необходимо выполнить упражнение 6.A.

Порядок выполнения упражнения

1. Войдите в домен под учетной записью пользователя, имеющего права администратора домена.
2. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **Политика безопасности домена**
3. Щелкните последовательно на **Параметры безопасности**, **Политики учетных записей**, **Политика паролей**.
4. Установите значение параметра **Мин. длина пароля** в ***8***, параметра **Мин. срок действия пароля** - в ***5***, параметра **Макс. срок действия пароля** - в ***60***.
5. Установите для параметра **Требовать неповторяемости паролей** значение ***12 хранимых паролей***.
6. Перейдите на закладку **Политика блокировки учетных записей**
7. Установите для параметра **Пороговое значение блокировки** значение ***5 ошибок входа в систему*** и нажмите **ОК** в окне **Предлагаемые изменения значений**, чтобы установить временные интервалы блокировки по умолчанию - ***30 минут***.
8. Закройте окно **Политика безопасности домена** и завершите сеанс текущего пользователя.
9. Используя учетную запись **vpupkin**, попробуйте 5 раз подряд войти в домен, вводя неправильный пароль, а затем введите правильный. Убедитесь, что система уже не дает войти данному пользователю.
10. Войдите в домен под учетной записью **admin** с паролем **adminpassword**.
11. Последовательно выберите **Пуск**, **Программы**, **Администрирование**, **Active Directory - пользователи и компьютеры**
12. Правой кнопкой щелкните на учетной записи **Василий Пупкин** и нажмите **Свойства**.
13. Убедитесь, что на закладке **Учетная запись** установлен флажок **Заблокировать учетную запись**. Снимите этот флажок и нажмите **ОК**.

Занятие 5: "Перемещения ролей хозяев операций"

Перемещение ролей хозяев операций на уровне всего леса

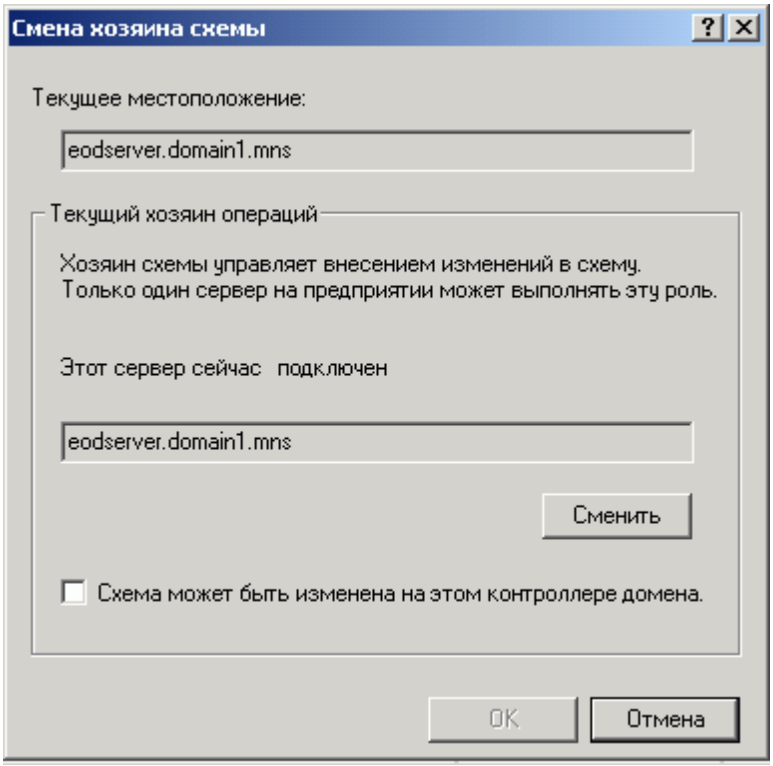
Каждый лес Active Directory должен содержать следующие роли.

- Хозяин схемы
- Хозяин именования домена

Перемещение роли хозяина схемы

Чтобы передать роль хозяина схемы, выполните следующие операции:

1. Откройте инструмент "Схема Active Directory".
2. В дереве консоли щелкните правой кнопкой мыши компонент **Схема Active Directory** и выберите команду **Изменение контроллера домена**.
3. Выберите режим **Любой контроллер**, чтобы служба Active Directory выбрала нового хозяина схемы, или выберите переключатель **Укажите имя** и введите имя компьютера для нового мастера схемы.
4. В дереве консоли щелкните правой кнопкой мыши компонент **Схема Active Directory** и выберите команду **Хозяин операций**.



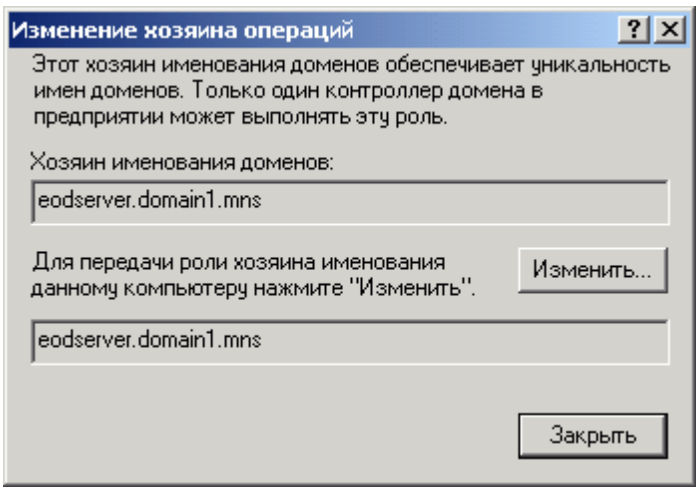
5. Нажмите **Сменить**.

Если схема Active Directory недоступна, необходимо установить средства администрирования Windows 2000 с компакт-диска Windows 2000 Server (файл adminpak.msi).

Перемещение роли хозяина именования домена

Чтобы передать роль хозяина именования домена, выполните следующие операции:

1. Откройте инструмент "Active Directory - домены и доверие".
2. В дереве консоли щелкните правой кнопкой контроллер домена, который будет новым хозяином именования домена, и выберите команду **Подключить к домену**.
3. Введите имя домена или нажмите кнопку **Обзор** и выберите домен из списка.
4. В дереве консоли щелкните правой кнопкой компонент **Active Directory - домены и доверие** и выберите команду **Хозяин операций**.



5. Нажмите **Изменить**.

Перемещение ролей хозяев операций на уровне домена

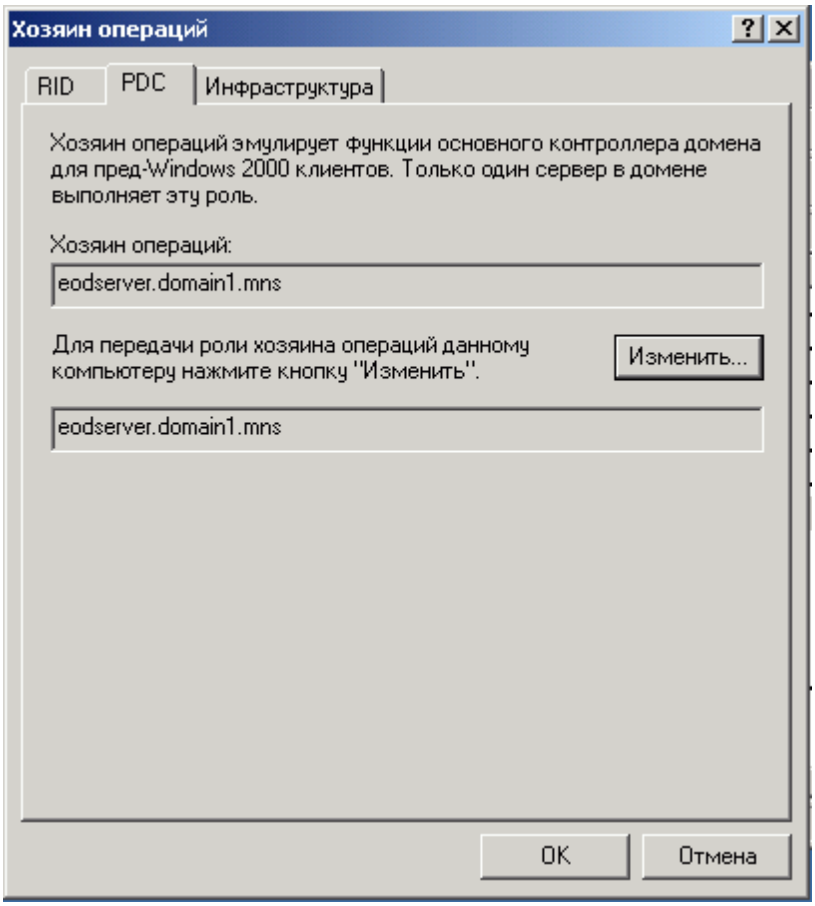
На уровне домена существуют три роли хозяина операций:

- Хозяин относительных идентификаторов
- Эмулятор основного контроллера домена
- Хозяин инфраструктуры

Для перемещения всех трех ролей используется инструмент "Active Directory — пользователи и компьютеры". Перемещение роли можно осуществить, только если существующий хозяин операций доступен по сети, иначе необходимо выполнять процедуру присвоения роли.

Чтобы передать роли, выполните следующие операции:

1. В дереве консоли щелкните правой кнопкой контроллер домена, который будет новым хозяином инфраструктуры, и выберите команду **Подключить к домену**.
2. Введите имя домена или нажмите кнопку **Обзор** и выберите домен из списка.
3. В дереве консоли щелкните правой кнопкой компонент **Active Directory — пользователи и компьютеры** и выберите команду **Хозяева операций**.
4. Выберите закладку **PDC** для перемещения роли эмулятора основного контроллера домена, закладку **RID** для роли хозяина относительных идентификаторов или закладку **Инфраструктура** для роли хозяина инфраструктуры.



5. Нажмите **Изменить**.

Присвоение ролей хозяев операций

Если сервер, выполняющий роль хозяина операций, в настоящий момент недоступен, то перемещение роли невозможно. В этом случае можно использовать ***присвоение роли***. Присвоение роли - радикальный метод, который должен применяться только в случае невозможности восстановления текущего хозяина операций.

Чтобы выполнить операцию присвоения роли серверу, выполните следующие операции:

1. Нажмите **Пуск**, выберите команду **Выполнить** и введите **cmd**.
2. В командной строке введите:**ntdsutil**.
3. В командной строке **ntdsutil** введите **roles**.
4. В командной строке **fsmo maintenance** введите **connections**.
5. В командной строке **server connections** введите **connect to server**, затем введите полное имя узла.
6. В командной строке **server connections** введите **quit**.
7. В командной строке **fsmo maintenance** в зависимости от того, какую роль надо присвоить, введите:
   - Для роли хозяина схемы - **seize schema master**
   - Для роли хозяина именования домена - **seize domain naming master**
   - Для роли хозяина относительных идентификаторов - **seize RID master**
   - Для роли эмулятора основного контроллера домена - **seize PDC**
   - Для роли хозяина инфраструктуры - **seize infrastructure master**
8. В командной строке **fsmo maintenance** введите **quit**.
9. В командной строке **ntdsutil** введите **quit**.

Немного в завершение курса

Итак, Вы открыли последнюю страницу этого курса. Он не всеобъемлющ, а содержит только базовый набор знаний по Windows 2000, требующий самостоятельной работы для полного освоения. Этот дистанционный курс разработан как дополнение к очным курсам, но не заменяет их. Выражаем надежду, что курс Вам понравился. Замечания и предложения присылайте по адресу educ@microinform.ru с темой "Дистанционный курс по Windows 2000".

Разработчик курса: преподаватель учебного центра "МИКРОИНФОРМ" Дмитрий Литвинов.

Учебный центр "МИКРОИНФОРМ"

На протяжении 15 лет МИКРОИНФОРМ признается специалистами лучшим российским учебным центром в области авторизованного обучения, первые авторизованные компанией Microsoft курсы по Windows NT прошли в 1994 году. По всем критериям МИКРОИНФОРМ - авторитетный, элитный учебный центр, обучение в котором является не только эффективным, но и престижным.

Подробнее о компании и проводимых курсах можно узнать на веб-сайте: www.microinform.ru.

Кратко о нововведениях в Windows Server 2003

Windows Server 2003 основана на технологиях, использованных в Windows 2000 Server. Это надежная и экономичная серверная операционная система. Ниже приведены основные изменения в Windows Server 2003 по сравнению с Windows 2000:

- **Усовершенствования службы Active Directory**

  В Windows Server 2003 появился целый ряд усовершенствований и новых возможностей: настройка доверия между лесами, возможность переименовывания доменов, улучшенные средства миграции с предыдущих версий служб каталогов, копирование данных репликации с компакт-диска или другого носителя как решение для установки контроллеров домена в удаленных офисах.
- **Консоль «Управление групповой политикой»**

  Администраторы могут использовать групповую политику для настройки параметров и определения действий пользователей и компьютеров. Управление на основе политик упрощает обновление системы, установку приложений и профилей пользователей, обеспечение требуемого уровня безопасности на рабочих станциях.

  Устанавливаемая как дополнительный компонент Windows Server 2003, консоль «Управление групповой политикой» (GPMC) предлагает новые возможности для централизованного управления компьютерами и пользователями: определение и анализ текущего набора политик, резервное копирование и восстановление, удаление, создание и перемещение.
- **Службы теневого копирования**

  Службы теневого копирования тома (VSS), иногда называемые «снимками», предоставляют инфраструктуру для создания копий одного или нескольких томов через определенные промежутки времени без прерывания работы служб. Эти копии впоследствии можно использовать для восстановления службы или архивирования. Пользователи могут получить архивные версии своих документов, которые, будучи невидимыми, хранятся на сервере.
- **Internet Information Services 6.0**

  Служба Internet Information Services (IIS) 6.0 - полнофункциональный веб-сервер, который позволяет использовать веб-приложения и веб-службы XML. IIS 6.0 полностью переработан на основе новой отказоустойчивой модели, которая значительно повышает надежность веб-узлов и веб-приложений.

  IIS также обеспечивает возможность наблюдения за состоянием веб-приложений: обнаружение неполадок, предотвращение сбоев и восстановление работы приложений. В Windows Server 2003 и Microsoft ASP.NET изначально применяется новая модель обработки для служб IIS. Эти расширенные возможности по наблюдению за состоянием приложений также доступны для работающих в среде Internet Information Server 4.0 и 5.0 приложений без дополнительной модификации.
- **Сервер электронной почты (POP3, SMTP)**

  Служба протокола POP3 (Post Office Protocol 3) обеспечивает передачу и получение электронной почты, а также управление учетными записями на почтовом сервере. Служба SMTP (Simple Mail Transfer Protocol) выполняет передачу сообщений электронной почты между серверами.

- **Интегрированное средство .NET Framework**

  Средство Microsoft .NET Framework является программной моделью приложений и технологий Microsoft .NET-connected. Оно используется для разработки, внедрения и выполнения веб-приложений и веб-служб XML, доступ к функциям которых осуществляется с помощью таких протоколов как SOAP, XML и HTTP. Полностью интегрированная в ОС Windows Server 2003 .NET Framework берет на себя заботу об интеграции и управлении, освобождая разработчиков от написания громоздкого кода.
- **Управление с помощью командной строки**

  В семействе продуктов Windows Server 2003 значительно усовершенствована инфраструктура командной строки, что позволяет администраторам выполнять большинство задач управления без использования графического интерфейса. Не менее важна возможность выполнять большое количество задач за счет доступа к хранилищам данных с помощью инструментария управления Windows (WMI) и командной строки WMI (WMIC).
- **Поддержка кластеров из восьми узлов**

  Эта служба, имеющаяся только в Windows Server 2003 Enterprise Edition и Windows Server 2003 Datacenter Edition, обеспечивает высокую доступность и масштабируемость важных приложений, таких как базы данных, системы обмена данными, а также файловые службы и службы печати. Поддержка кластеров осуществляется за счет постоянного подключения к друг другу нескольких серверов (узлов). Если один из узлов кластера в результате сбоя или ремонтных работ становится недоступным, другой узел немедленно приступает к обслуживанию (этот процесс называется перемещением при сбое). Пользователи, которые получают доступ к определенной службе, продолжают работать, не подозревая, что она поддерживается уже с другого сервера (узла).

  В Windows Server 2003 Enterprise Edition и Windows Server 2003 Datacenter Edition поддерживаются кластеры, включающие до восьми узлов.
- **Безопасные беспроводные локальные сети (802.1x)**

  С появлением в семействе продуктов Windows Server 2003 поддержки стандарта 802.1x компании могут использовать безопасную модель доступа, которая гарантирует проверку подлинности и шифрование данных для всех подключений к сети. Использование оборудования точек доступа и маршрутизаторов стандарта 802.1X позволяет проверять подлинность всех подключающихся систем и обмениваться данными с защищенными сетями. Поскольку в беспроводных сетях стандарта 802.1X используется динамическое определение ключей, шифрование данных в них значительно более надежно, чем аналогичные операции с использованием ключей WEP в сетях IEEE 802.11.
- **Службы аварийного управления: поддержка сервера без монитора**

  Эта функция позволяет администраторам устанавливать ПО и управлять компьютером без использования монитора, видеоадаптера, клавиатуры и мыши. Новые службы аварийного управления помогают выполнять удаленное управление и восстановление системы даже в тех случаях, когда недоступны другие стандартные средства и механизмы удаленного администрирования.