ОПЕРАЦИОННЫЕ СИСТЕМЫ

Часть 2

ОПЕРАЦИОННАЯ СИСТЕМА WINDOWS 2000 PROFESSIONAL.

КОНСОЛИ УПРАВЛЕНИЯ. ТИПОВЫЕ ЗАДАЧИ АДМИНИСТРИРОВАНИЯ

Для студентов всех форм бучения

Специальности:

220200 – Автоматизированные системы обработки информации и управления

220100- Вычислительные машины, комплексы, сети и системы

071900 – Информационные системы и технологии

Екатеринбург 2004

УДК 681.3.06

Составитель О.М. Зверева

Научный редактор: д-р техн. наук Л.Г. Доросинский

Операционные системы. Ч. 2. Операционная система Windows 2000 Professional. Консоли управления. Типовые задачи администрирования. / О.М. Зверева. Екатеринбург, 2004, 99с.

В работе описан процесс создания нового инструмента для администрирования операционных систем Windows 2000 – консоли управления. Подробно описана работа с консолью Управление компьютером для решения основных задач администрирования системы. Рассмотрен один из аспектов обеспечения безопасности данных в системе – применение шифрующей файловой системы

Библиогр .: 4 назв. Табл. 6. Рис. 30.

Подготовлено кафедрой «Автоматизированные системы управления»

7. СРЕДСТВА УПРАВЛЕНИЯ

Общие концепции консоли управления Microsoft

В Windows 2000 был кардинально изменен интерфейс управления операционной системой. В соответствии с новой концепцией Microsoft из системы Windows NT были удалены все автономные и несовместимые друг с другом административные утилиты и разработана единая среда управления, получившая название *консоль управления Microsoft* (Microsoft Management Console, MMC). Эта общая консоль управления разработана для запуска всех программных модулей администрирования, конфигурирования или мониторинга локальных компьютеров и сети в целом. Такие законченные модули называются *оснастками* (snap-in). Консоль управления сама по себе не выполняет никаких функций администрирования, но служит в качестве рабочей среды для запуска оснасток, создаваемых как компанией Microsoft, так и независимыми поставщиками программного обеспечения (Independent Software Vendor,ISV).

Появление MMC обусловлено желанием создать единую среду управления для администрирования операционных систем Windows. Оснастки представляют собой управляющие компоненты, которые объединены в среде MMC. Из нескольких оснасток можно создать индивидуальный управляющий инструмент.

Консоль MMC включает в себя интерфейсы прикладного программирования (API), оболочку пользовательского интерфейса (консоли) и набор инструкций.

Microsoft Management Console позволяет создавать более совершенные административные инструменты, которые могут предоставлять различные уровни функциональных возможностей. Эти инструменты можно легко интегрировать в операционную систему, а также изменять и настраивать по своему усмотрению. В данном случае инструмент представляет собой не просто одиночное приложение. Инструмент может состоять из одной или нескольких оснасток, и каждая оснастка, в свою очередь, может содержать дополнительные оснастки расширения. Такая модульная структура позволяет системному администратору существенно снизить стоимость управления системой благодаря возможности создания индивидуальных инструментов на основе выбранных оснасток, которые предоставляют только необходимые возможности и средства просмотра. Администратор может затем сохранять каждый индивидуальный инструмент в отдельном файле (файле консоли MMC с расширением .msc) и отправлять его другим

пользователям или администраторам, которым делегированы права на выполнение данных административных задач.

MMC и модель администрирования Windows 2000 представляют собой следующий шаг в развитии технологий администрирования. Консоль управления имеет ряд преимуществ, которые заключаются в упрощении интерфейса, предоставлении больших возможностей по настройке разработанных решений для определенных административных проблем и в обеспечении различных уровней функциональности. В большинстве случаев достаточно сложно разработать инструмент, который будет являться неотъемлемой частью операционной системы. С помощью MMC эта задача существенно упрощается. Тщательно разработанный административный инструмент идеально подойдет для решения стоявших перед вами задач и будет иметь интуитивно понятный интерфейс. Такой инструмент также будет использовать возможности уже имеющихся инструментов, что снимает необходимость «изобретать велосипед».

В операционные системы Windows 2000 и следующие версии продуктов семейства BackOffice оснастки MMC включены в качестве стандартных административных программ.

Что такое MMC? Microsoft Management Console представляет собой приложение с многооконным интерфейсом, которое активно использует технологии Интернет. Компания Microsoft и независимые поставщики программного обеспечения могут разрабатывать оснастки MMC для выполнения задач управления локальным компьютером и сетью в целом.

Интерфейсы программирования MMC позволяют интегрировать оснастки с консолью (рис. 1). Данные интерфейсы предоставляют только расширения пользовательского интерфейса, поскольку каждая оснастка самостоятельно определяет механизм выполнения своих задач. Интерфейсы MMC позволяют оснасткам совместно использовать хост-среду и обеспечивают интеграцию между приложениями. Консоль MMC не выполняет никаких функций управления.

Компания Microsoft и независимые поставщики программного обеспечения могут разрабатывать инструменты управления для запуска в среде MMC и приложения, которыми будут управлять инструменты MMC.

Инструменты, не предназначенные для работы в среде MMC, могут быть интегрированы в MMC посредством оснасток или запущены независимо. Системный администратор может одновременно запускать

не-MMC инструменты управления и экземпляры MMC на одном компьютере.

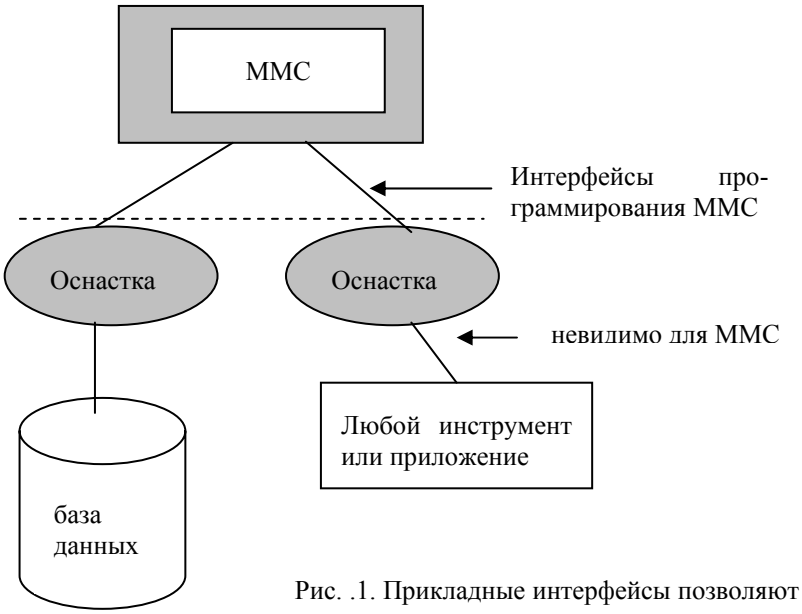

Рис. .1. Прикладные интерфейсы позволяют интегрировать оснастки с консолью

Преимущества MMC

- Возможность индивидуальной настойки и передача полномочий.

Помимо обеспечения интеграции и общей среды для административных инструментов, консоль MMC предоставляет возможность полностью индивидуальной настройки, так что администраторы могут создавать такие консоли управления, которые будут включать только необходимые им инструменты. Такая настройка позволяет ориентировать администрирование на выполнение конкретных задач, причем администратор может выделить только необходимые объекты и элементы.

Настройка консоли также позволяет администраторам передавать определенную часть полномочий менее опытным сотрудникам. С помощью MMC можно создать консоль, которая будет содержать объекты, необходимые для выполнения только определенных функций.

- Интеграция и унификация

MMC обеспечивает общую среду, в которой могут запускаться оснастки, и администраторы могут управлять различными сетевыми продуктами, используя единый интерфейс, что упрощает изучение работы с различными инструментами.

- Гибкость в выборе инструментов и продуктов

В среде MMC можно использовать различные инструменты и оснастки. Для использования в среде MMC оснастка должна поддерживать объектную модель компонентов (Component Object Model, COM) или распределенную COM (Distributed Component Object Model, DCOM). Это позволяет выбирать наиболее оптимальный продукт среди оснасток, причем гарантируется его полная совместимость со средой MMC.

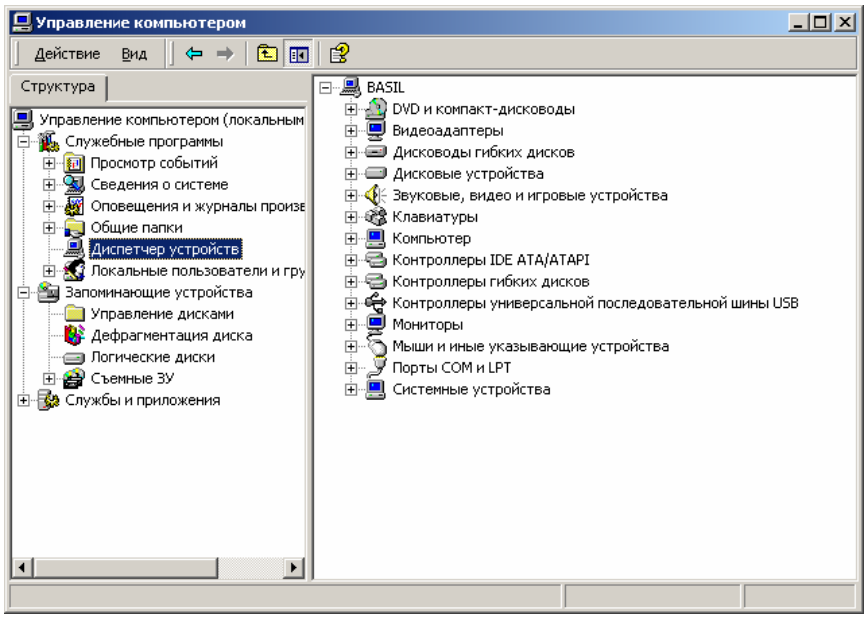

Рис. 2. Окно оснастки **Управление компьютером**

Пользовательский интерфейс MMC

Консоль управления MMC имеет пользовательский интерфейс, позволяющий открывать множество документов (Multiple Document Interface, MDI). Интерфейс консоли MMC на примере оснастки **Управление компьютером** показан на рис. 2.

Родительское окно MMC имеет главное меню и панель инструментов. Главное меню обеспечивает функции управления файлами и окнами, а также доступ к справочной системе.

Дочерние окна MMC представляют собой различные средства просмотра автономного документа консоли. Каждое из этих дочерних окон содержит панель управления, панель структуры (scope panel) и панель результатов, или сведений (result panel). Панель управления содержит меню и набор инструментов. Панель структуры отображает пространство имен инструментов в виде дерева, которое содержит все видимые узлы, являющиеся управляемым объектом, задачей или средством просмотра.

Панель результатов в дочернем окне отображает список элементов выбранного узла. Данный список может содержать папки, оснастки, элементы управления, веб-страницы, панели задач (taskpad) и другие элементы.

Средства MMC также позволяют отображать окно в упрощенном виде, доступном для менее опытных администраторов. В наиболее простой форме окно может содержать набор значков, которые обеспечивают доступ к определенным задачам.

Архитектура MMC

На рис. 3 представлена архитектура MMC.

Диспетчер оснасток (Snap-in Manager) дает системному администратору или разработчику оснасток возможность добавлять, удалять или изменять оснастки. Кроме того, Диспетчер оснасток позволяет системному администратору определить, является ли некоторая оснастка изолированной или зависит от других оснасток.

Диспетчер оснасток сохраняет произведенные установки в виде *инструмента* или *документа* (файл с расширением .msc). Пользователь определенного инструмента взаимодействует с элементами, которые находятся в верхней части рисунка (файл *.msc и элементы пользовательского интерфейса). Разработчики и администраторы работают с элементами, показанными в нижней части рис. .3 (Диспетчер оснасток и оснастки **Просмотр событий** и **Маршрутизация н удаленный доступ).**

При загрузке документа MMC инициализируется одна или несколько оснасток, как показано на рис. 4.

Рис. 3. Модель MMC (файл *.msc взаимодействует с диспетчером оснасток для извлечения оснасток и представления элементов пользовательского интерфейса

Данные оснастки объединены для создания пространства имен – набора узлов, которые отображаются в виде дерева на панели структуры. Пространство имен является главным деревом, которое показывает возможности инструмента. Пространство имен может включать все управляемые объекты сети - компьютеры, пользователей, группы и т. д. Пространство имен содержит объекты, средства просмотра и задачи. Дочерние окна MMC представляют собой средства просмотра главного пространства имен.

Оснастки и работа с ними

Все инструменты MMC состоят из совокупности оснасток. Каждая оснастка представляет собой минимальную единицу управления. С технической стороны оснастка представляет собой «OLE-сервер внутри процесса», который выполняется в контексте процесса MMC. Оснастка может вызывать другие элементы управления и динамические

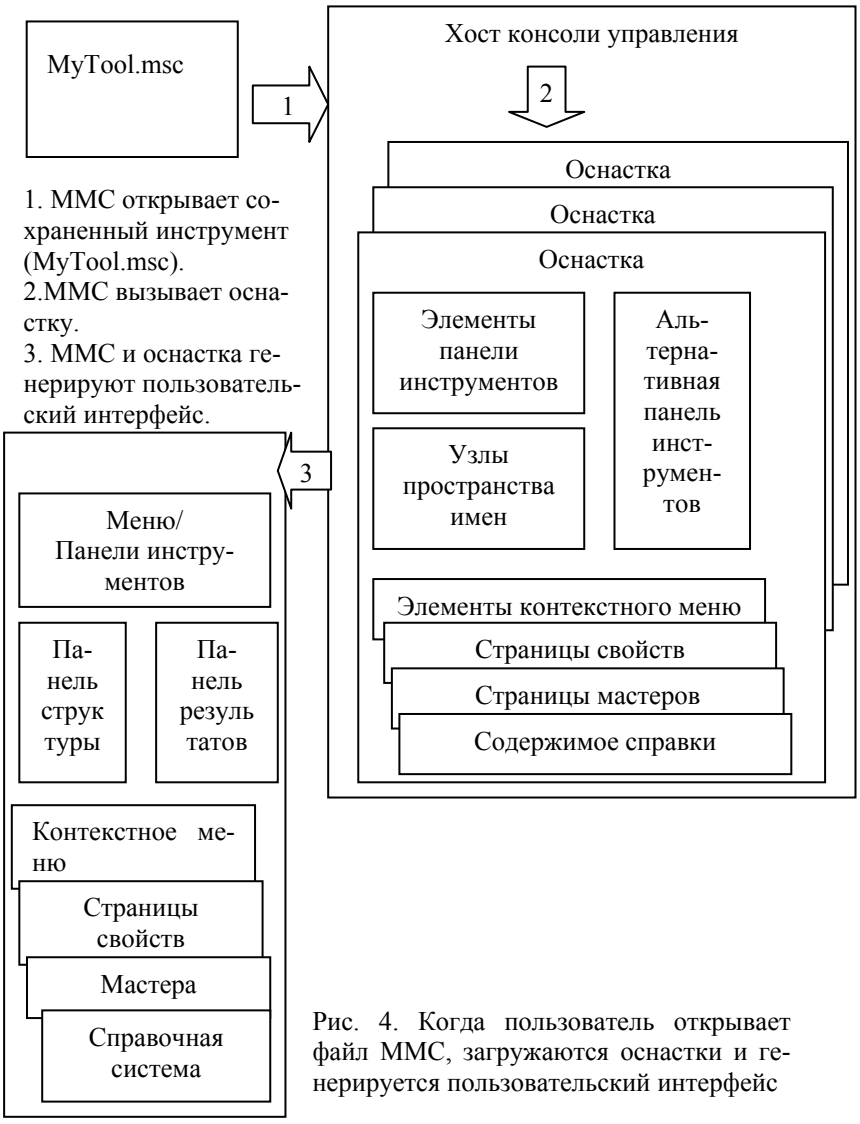

Рис. 4. Когда пользователь открывает файл ММС, загружаются оснастки и генерируется пользовательский интерфейс

библиотеки (DLL) для выполнения своей задачи.

Несколько оснасток могут быть объединены администратором *в инструмент* (также называется *документом),* который сохраняется в файле с расширением .msc (Management Saved Console). Этот файл можно затем передать другому администратору (например, по электронной

почте), который сможет использовать содержащийся в нем инструмент на своем рабочем месте.

Примечание. На практике термины *инструмент* и *оснастка* иногда могут использоваться как взаимозаменяемые, поскольку некоторые инструменты MMC (и стандартные, и вновь созданные) содержат только одну оснастку. С другой стороны, термин *оснастка* применяется чаще, так как именно в оснастке реализованы все функциональные возможности, а включаться она может в различные инструменты – в том числе и в те, которые конфигурирует сам администратор. Поэтому чаще можно встретить фразу: «Данная функция реализуется при помощи оснастки...» (а не «при помощи инструмента...»).

Благодаря возможности индивидуальной настройки MMC, администратор может создать идеальный инструмент на основе доступных оснасток. Каждый инструмент может иметь множество функций: например, возможности управления службой Active Directory, топологией репликации, доступом к файлам и т. д. В больших сетях администраторы могут иметь набор инструментов, организованных по категориям выполняемых с их помощью задач.

Типы оснасток

В MMC поддерживаются два типа оснасток:

Изолированная оснастка (standalone snap-in) обеспечивает выполнение своих функций даже при отсутствии других оснасток, например, **Управление компьютером** (Computer management).

Оснастка расширения (extension snap-in) может работать только после активизации родительской оснастки. Функция оснастки расширения заключается в увеличении числа типов узлов, поддерживаемых родительской оснасткой. Оснастка расширения является подчиненным элементом узлов определенных типов, и при каждом запуске узлов данных типов консоль автоматически запускает все связанные с ней расширения. В качестве примера можно привести оснастку **Диспетчер устройств** (Device Manager). Оснастки расширения могут предоставлять различные функциональные возможности. Например, такие оснастки могут расширять пространство имен консоли, увеличивать число пунктов в меню или добавлять определенные мастера.

Создание новой консоли

Для того чтобы получить представление о гибкости MMC, полезно рассмотреть процесс создания файла консоли – инструмента (документа) MMC – с самого начала. Для примера опишем процедуру

создания новой консоли и добавления к ней оснасток **Управление компьютером** и **Сертификаты** (Certificates).

1. В меню **Пуск** выберите пункт **Выполнить**, введите **mmc** и нажмите кнопку ОК. Откроется окно **Консоль1** с пустой *консолью* (или *административным инструментом).*

Примечание. По умолчанию консоль MMC открывается в *авторском режиме,* в котором можно создавать новые консоли и изменять созданные ранее административные инструменты. Пустая консоль не имеет никаких функциональных возможностей до тех пор, пока в нее не добавлены оснастки. Команды меню MMC на панели меню в верхней части окна применимы ко всей консоли.

2. В меню **Консоль** (Console) выберите пункт **Добавить/удалить оснастку** *(*Add/Remove Snap-in). Откроется окно **Добавить/Удалить оснастку.** В этом окне перечисляются изолированные оснастки и оснастки расширения, которые будут добавлены в консоль (или уже включены в нее). Оснастки можно добавлять к корню консоли управления или к уже имеющимся изолированным оснасткам (другим узлам дерева); это указывается в списке **Оснастки** (Snap-in added to). В нашем случае оставим значение по умолчанию – **Корень консоли** (Console Root).

3. Нажмите кнопку **Добавить** *(*Add*).* На экране появится окно **Добавить изолированную оснастку** (Add Standalone Snap-in) (рис. 5) со списком изолированных оснасток, имеющихся в системе.

4. Выполните двойной щелчок на пункте **Управление компьютером.** Появится окно с конфигурационными опциями для данной оснастки.

5. Оставьте переключатель в положении **локальным компьютером** (Local Computer). Затем нажмите кнопку **Готово** (Finish).

6. В окне оснасток выберите пункт **Сертификаты** и нажмите кнопку **Добавить**.

7. В следующем окне выберите соответствующий переключатель – **Эта оснастка всегда будет управлять сертификатами для**:

    - **моей учетной записи пользователя** (My user account);
    - **учетной записи службы** (Service account);
    - **учетной записи компьютера** (Computer account).

Нажмите кнопки **Готово** и **Закрыть**.

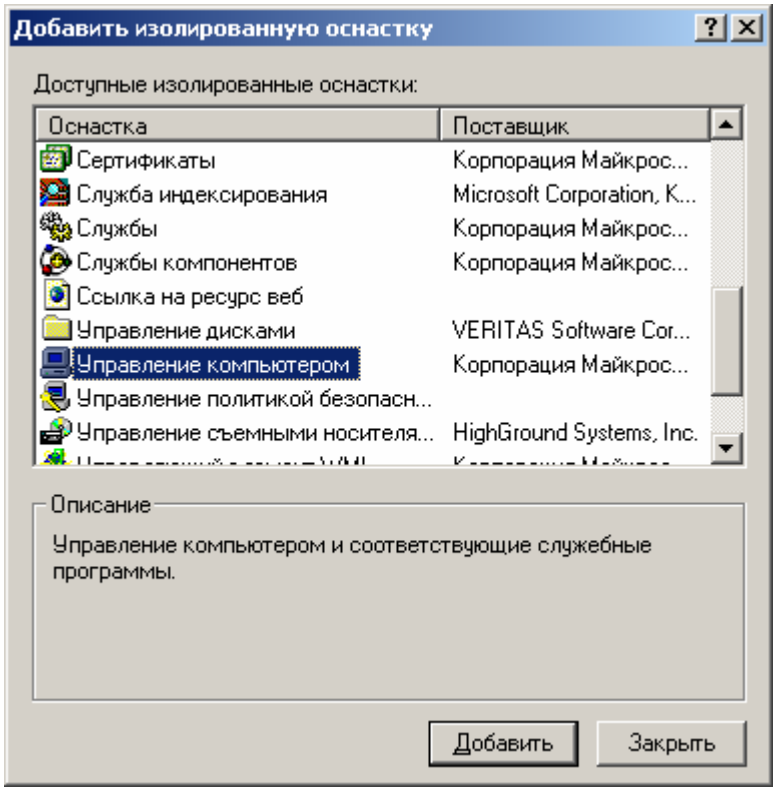

Рис. 5. Окно со списком имеющихся оснасток

8. В окне **Добавить/Удалить оснастку** (где отображен список подключаемых оснасток) перейдите на вкладку **Расширения** (Extensions). На этой вкладке приведен список оснасток расширения, которые поставляются вместе с выбранными изолированными оснастками. Если вы не собираетесь подключать все оснастки расширения, сбросьте флажок **Добавить все расширения** (Add All Extensions) (который ставится по умолчанию) и снимите флажки с лишних оснасток. По окончании процедуры нажмите кнопку **ОК**.

9. Закройте окно добавления оснасток, нажав кнопку **ОК**. Теперь окно консоли содержит две оснастки – **Управление компьютером** и **Сертификаты**.

10. Для того чтобы сохранить созданный инструмент, в меню **Консоль** выберите пункт **Сохранить как** (Save As) и укажите имя файла и папку, в которой будет сохранен файл консоли.

Примечание. Дополнительным преимуществом такого подхода является то, что при наличии у пользователя перемещаемого (блуждающего) профиля, все созданные пользователем инструменты будут перемещаться вместе с ним.

Индивидуальная настройка окон оснасток

После добавления оснасток можно развернуть окна оснасток, чтобы облегчить работу с ними. Для этого выполните следующие действия:

1. В левом подокне (в окне структуры) только что созданной консоли щелкните правой кнопкой мыши на узле **Управление компьютером** и выберите в контекстном меню **Новое окно отсюда** (New Window from Here). Будет открыто окно **Управление компьютером**, представляющее одноименную оснастку.

2. Аналогичные действия выполните для узла **Сертификаты.** В но-

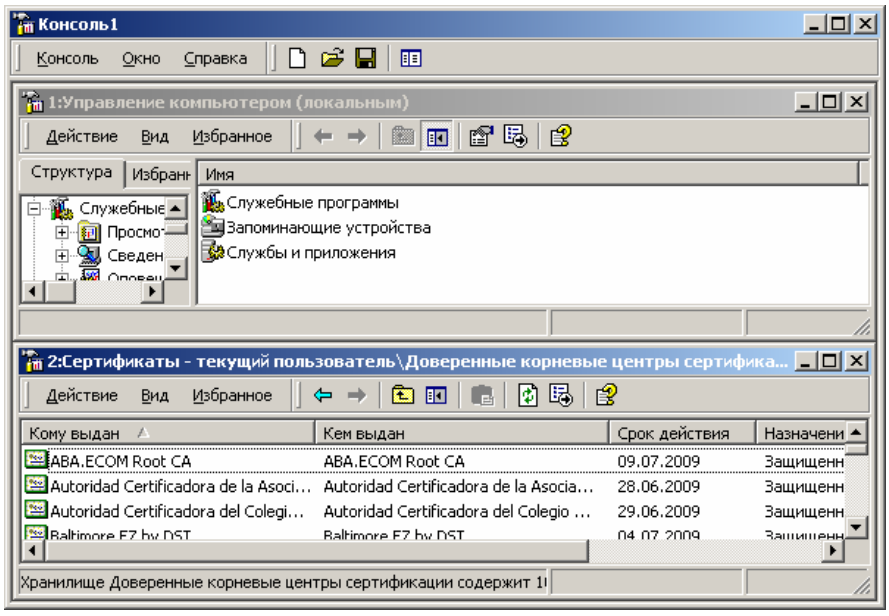

Рис. 6. Окно консоли с индивидуальной настройкой

вом окне нажмите кнопку **Скрытие или отображение дерева консоли или избранного** (Show/Hide Console tree) на панели инструментов для того, чтобы скрыть панель структуры.

3. Закройте окно , содержащее корень консоли.

4. В меню **Окно** (Window) выберите команду **Сверху вниз** (Tile Horizontally). Консоль будет выглядеть, как показано на рис. 6.

Примечание. Дочерние окна в окне консоли имеют панель инструментов с кнопками и раскрывающимися меню. Кнопки и команды этих меню применяются только к содержанию соответствующего окна.

Создание панелей задач

Когда требуется создать файл консоли для другого пользователя, полезно предоставить пользователю упрощенный инструмент, позволяющий выполнять только несколько определенных задач. Таким инструментом является панель задач (taskpad). Панель задач является HTML-страницей, на которой могут быть размещены ярлыки (или задачи (tasks)), запускающие команды меню и программы или открывающие ссылки на веб-страницы.

Для создания панели задач выполните следующее:

1. В меню **Действие** (Action) или в контекстном меню любого узла в окне консоли выберите пункт **Новый вид панели задач** (New Taskpad View).

2. Откроется окно Мастера создания вида панели задач (New Taskpad View Wizard). Нажмите кнопку **Далее**.

3. В следующем окне мастера вам будет предложено выбрать стиль отображения и размер панели задач (рис. 7). Затем на панели задач вы можете указать использование только тех задач, которые связаны с текущим узлом или со всеми узлами дерева. В следующем окне потребуется ввести имя и описание создаваемой панели задач.

4. Если вы не собираетесь пока добавлять новые задачи на созданную панель, снимите в последнем окне мастера флажок **Запустить мастер создания новой задачи** (Start New Task Wizard).

5. В противном случае по завершении работы Мастера создания вида панели задач запускается Мастер создания задач (New Task Wizard). В ходе этой процедуры следует указать функцию задачи: запуск команды меню, программы или ссылка на веб-

страницу, ввести путь к исполняемому файлу и параметры запуска.

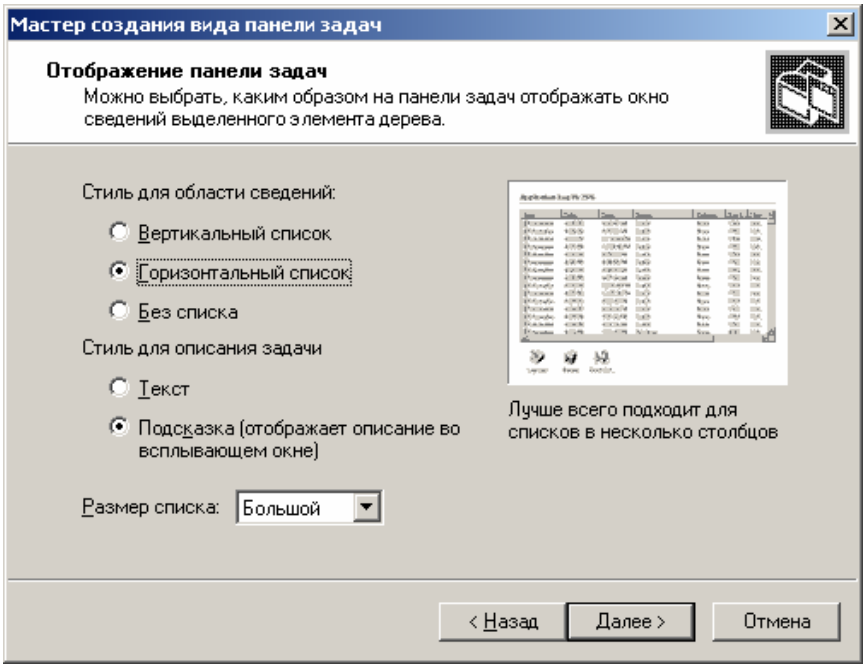

Рис. 7. Окно мастера создания панелей

6. Если новая задача будет запускать команду меню, в следующем окне будет предложено указать элементы в панели результатов, к которым будет применяться выбранная команда. Например, при создании панели задач для просмотра событий в системе это окно выглядит, как показано на рис. 8.

7. В остальных окнах мастера примите значения по умолчанию. Если требуется создать несколько задач на одной панели, установите в последнем окне мастера флажок **Запустить этот мастер снова** (Run this wizard again). Затем нажмите кнопку **Готово**.

8. На рис. 9 показана созданная в результате панель задач. В данном окне консоли панель структуры отключена – аналогично тому, как это было сделано в предыдущем разделе. Для удаления лишних меню и панелей инструментов снимите соответствующие флажки в окне **Настройка вида** (Customize View) (опции

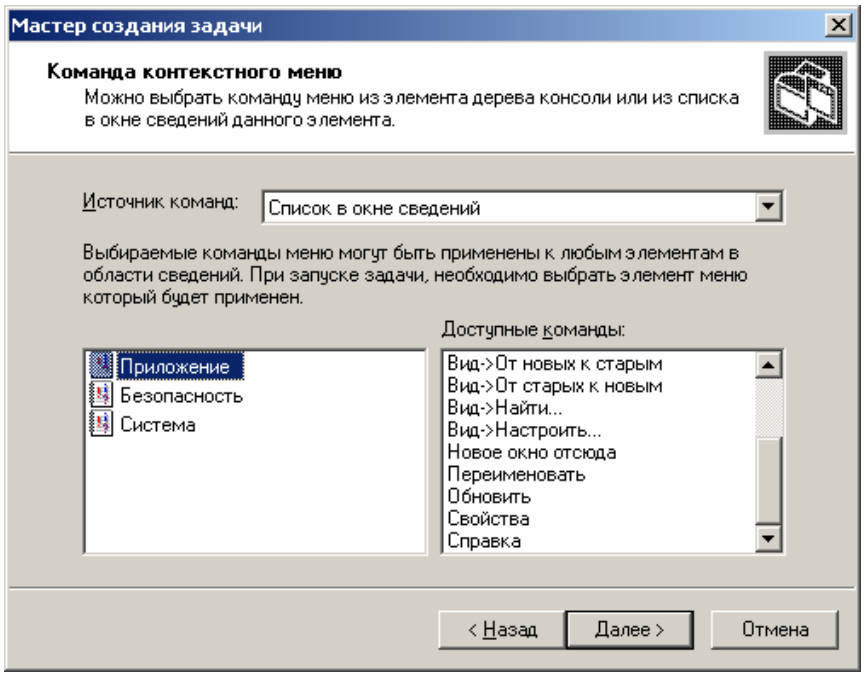

Рис. 8. Окно выбора элемента узла и команды, которые будут к нему применяться

Вид (View) | **Настроить** (Customize) на панели инструментов или команда **Вид** | **Настроить** в контекстном меню созданной панели задач).

Примечание. Функция Новый вид панели задач доступна только в окне индивидуальной консоли. В стандартных оснастках эта функция отсутствует.

Установка опций консоли

Если консоль создается для другого пользователя, может оказаться полезным установить запрет на изменение консоли. Для этого следует открыть окно **Параметры** (Options).

1. В меню **Консоль** выберите пункт **Параметры** (Options) (рис. 10).
2. Установите в списке **Режим консоли** (Console mode*)* значение **Пользовательский режим – полный доступ** (User Mode – full access). В этом режиме пользователь не сможет добавлять новые

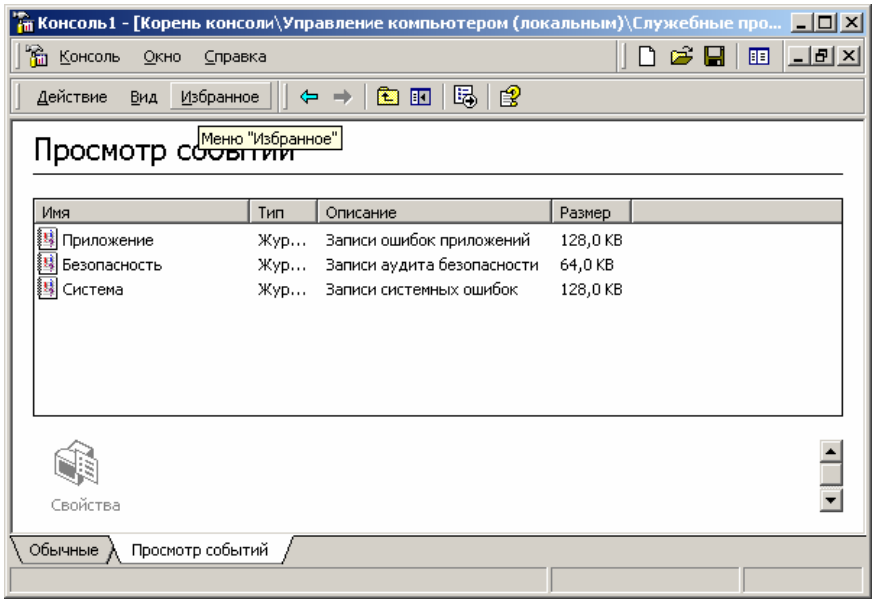

Рис. 9. Окно консоли с панелью задач

оснастки в инструмент или удалять существующие, не сможет изменять свойства консоли, но будет иметь возможность изменять расположение окон. (Новый режим начнет работать при следующем запуске файла консоли). Если вы хотите еще ужесточить требования, то можете выбрать один из режимов ограничения **– Пользовательский режим –ограниченный допуск**.

3. Нажмите кнопку **OK** и сохраните файл.

Сохраненный файл консоли можно также открыть с помощью Проводника. Для этого выполните двойной щелчок на файле с расширением .msc. Файл консоли будет открыт в среде MMC.

Запуск инструментов MMC

Для запуска стандартных инструментов MMC, установленных на компьютере, можно использовать один из приведенных ниже способов:

- Откройте меню **Пуск** | **Программы** | **Администрирование** (Start | programs | Administrative Tools) и выберите необходимый инструмент.

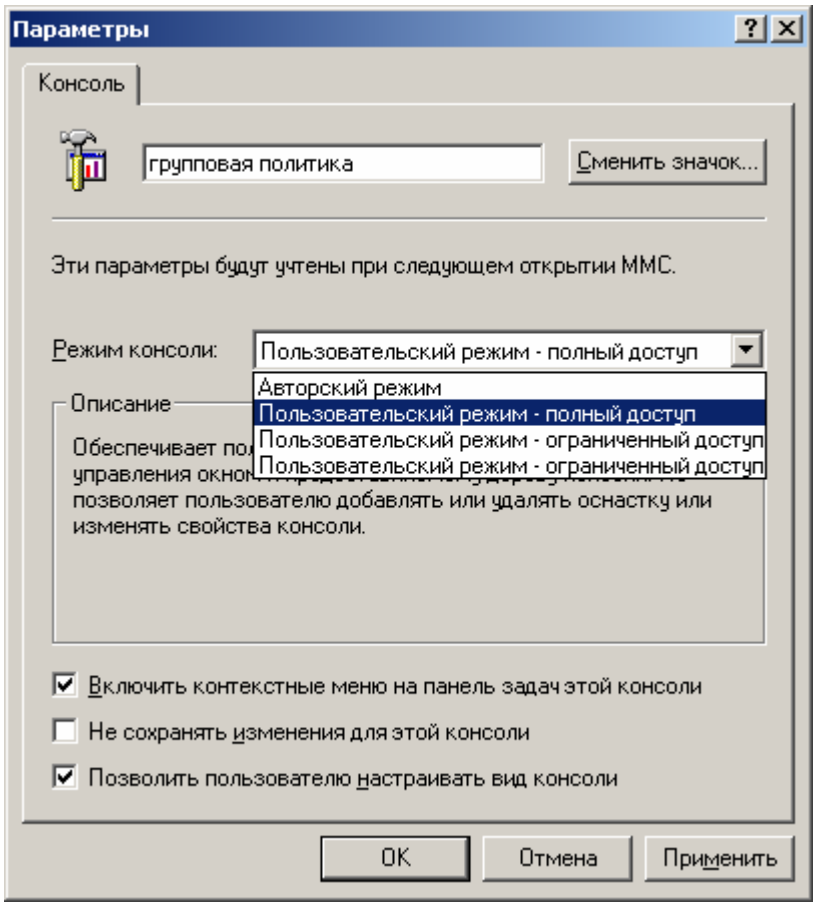

Рис. 10. Окно установки опций консоли

- Дважды щелкните на значке **Администрирование** на панели управления. Откроется окно **Администрирование,** содержащее значки всех установленных на компьютере инструментов.

Оснастки Windows 2000

В табл. 1 в алфавитном порядке перечислены основные оснастки, которые доступны в системе Windows 2000 Professional. Для оснасток, включенных в пользовательский интерфейс, указаны названия соответствующих пунктов меню, для остальных оснасток даны их собственные имена. Оснастки, которые можно вызывать непосредственно

из меню **Пуск** или из группы **Администрирование** на панели управления, т.е. оснастки, включенные в пользовательский интерфейс при инсталляции системы, - отмечены звездочкой (*).

Оснастки Windows 2000 Professional

Таблица 1

Оснастка	Назначение
Служба работы с факсами (Fax Service Management)	Служит для управления службой и устройствами факсимильной связи
Анализ и настройка безопасности (Security Configuration and Analysis)	Служит для управления безопасностью системы с помощью шаблонов безопасности
Групповая политика (Group Policy)	Служит для назначения сценариев регистрации, групповых политик для компьютера и пользователей некоторого компьютера сети; позволяет просматривать и изменять политику безопасности, политику аудита и права пользователей
Дефрагментация диска (Disk Defragmenter)	Служит для анализа и дефрагментации дисковых томов
Диспетчер устройств (Device Manager)	Содержит список всех устройств, подключенных к компьютеру, и позволяет их конфигурировать
Локальные пользователи и группы (Local Users and Groups)	Служит для управления локальными учетными записями пользователей и групп
Общие папки Shared Folders)	Отображает совместно используемые папки, текущие сеансы и открытые файлы
Оповещение и журналы производительности (Performance Logs and	Конфигурирует журналы данных о работе системы и службу оповещений

Оснастка	Назначение
Alerts)	
Папка (Folder)	Служит для добавления новой папки в дерево
Просмотр событий (Event Viewer)*	Служит для просмотра и управления системным журналом, журналами безопасности и приложений
Сведения о системе (System Information)	Отображает информацию о системе
Сертификаты (Certificates)	Служит для управления сертификатами
Системный монитор (Performance)*	Используется для сбора и просмотра в реальном времени данных, характеризующих работу памяти, дисков, процессора и других компонентов системы
Служба индексирования (Indexing Service)	Служит для индексирования документов различных типов с целью ускорения их поиска
Служба компонентов (Componenet Services)*	Конфигурирует и управляет службами компонентов COM+
Службы (Services)*	Запускает, останавливает и конфигурирует службы (Services) Windows
Ссылка на ресурс веб (Link to Web Address)	Служит для подключения веб-страниц (html, asp, stml)
Управление дисками (Disk Management)	Служит для управления дисками и защитой данных, для разбиения дисков на логические тома, форматирования, управления совместным доступом, квотами и т. д.
Управление компьютером (Computer Management)*	Предоставляет функции администрирования системы. Содержит в своем составе ряд изолированных оснасток и оснасток

Оснастка	Назначение
	расширения
Управление политикой безопасности IP (IP Security Policy Management)	Служит для управления политиками IPSec для безопасного соединения с другими компьютерами
Управлене съемными носителями (Removable Storage Management)	Служит для управления съемными носителями информации
Управляющий элемент (WMI Control)	Служит для конфигурирования средств Windows Management Instrumentation и управления ими
Шаблоны безопасности (Security templates)	Обеспечивает возможность редактирования файлов-шаблонов безопасности
Элемент ActiveX (ActiveX Control)	Подключение к дереву консоли различных элементов управления ActiveX

8. УПРАВЛЕНИЕ КОМПЬЮТЕРОМ

Инструмент (и одноименная оснастка) **Управление компьютером** (рис. 2) является одним из основных средств системного администратора для конфигурирования компьютера. Данную оснастку можно использовать для администрирования как локальной системы, так и удаленных компьютеров (в том числе - с некоторыми ограничениями - и компьютеров с Windows NT 4.0). Это позволяет администратору со своего рабочего места устранять проблемы и конфигурировать любой компьютер в сети, на котором установлена Windows 2000.

Для запуска оснастки **Управление компьютером** можно пользоваться двумя вариантами: выбрать соответствующий значок в группе **Администрирование** на панели управления или щелкнуть правой кнопкой мыши на значке **Мой компъютер** (My Computer*)* на рабочем столе и выбрать в контекстном меню пункт **Управление** (Manage).

Примечание. Когда в системе доступно меню **Администрирование**, можно воспользоваться меню **Пуск** | **Программы** | **Администрирование** | **Управление компьютером**.

В пространстве имен оснастки имеются три узла: **Служебные программы** (System Tools), **Запоминающие устройства** (Storage) и **Службы и приложения** (Services and Applications). Данные узлы являются контейнерами и содержат ряд оснасток:

- **Служебные программы** – узел содержит инструменты, предназначенные для администрирования компьютеров Windows 2000. В данный узел входят:
    - Просмотр событий (Event Viewer*)*
    - Сведения о системе *(*System Information)
    - Оповещения и журналы производительности (Performance Logs and Alerts)
    - Общие папки (Shared Folders)
    - Менеджер устройств (Device Manager)
    - Локальные пользователи и группы (Local Users and Groups)
- **Запоминающие устройства** - узел содержит оснастки, служащие для управления дисками:
    - Управление дисками (Disk Manager)
    - Дефрагментация диска (Disk Defragmenter)
    - Логические диски (Logical Drives)
    - Съемные ЗУ *(*Removable Storage)
- **Службы и приложения -** узел содержит следующие оснастки:
    - Управляющий элемент WMI (%M1 Соп1го1)
    - Службы (Services)
    - Служба индексирования (Indexing Service)
    - Другие оснастки - в зависимости от того, какие дополнительные службы установлены в системе

Служебные программы (System Tools)

Узел **Служебные программы** отображает конфигурацию компьютера и объединяет средства управления им. Сотрудники службы

поддержки используют данную информацию при устранении проблем на локальном компьютере.

Просмотр событий (Event Viewer)

Узел **Просмотр событий** соответствует оснастке с одноименным названием и стандартной утилите, которая имеется в Windows NT 4.0. С ее помощью можно просматривать журналы регистрации событий операционной системы, безопасности и приложений.

Сведения о системе (System Information)

Узел **Сведения о системе** содержит исчерпывающую информацию об аппаратном обеспечении компьютера, системных компонентах и программной среде. Системная информация разделена на четыре категории, которым соответствуют узлы **Сведения о системе** (System Information), **Ресурсы аппаратуры** (Hardware Resources), **Компоненты** (Components) и **Программная среда** (Software Environment) на панели структуры:

- Узел **Сведения о системе** отображает общую информацию о компьютере и операционной системе: версию ОС и номер сборки, тип процессора, объем ОЗУ; версию BIOS, региональные установки, а также информацию об объеме физической и виртуальной памяти на компьютере.
- Узел **Ресурсы аппаратуры** отображает информацию об аппаратных установках, таких как каналы DMA, номера прерываний (IRQ), адреса ввода/вывода (I/O) и адреса памяти. Узел **Конфликты/Совместное использование** (Conflicts/Sharing) идентифицирует устройства, которые совместно используют ресурсы или конфликтуют с другими ресурсами. Такая информация помогает выявлять проблемы, возникающие с аппаратными устройствами.
- Узел **Компоненты** отображает информацию о конфигурации Windows и используется для определения статуса драйверов устройств, сетевых устройств и программного обеспечения мультимедийных устройств. Кроме того, данный узел содержит обширную информацию об истории драйверов с записью всех изменений, которые производились с компонентами.
- Узел **Программная среда** отображает «снимок» программного обеспечения, загруженного в память компьютера. Данная информация может быть использована для просмотра списка выполняющихся задач или для выяснения номера версии продукта.

В узел **Сведения о системе** другими приложениями могут быть добавлены узлы с целью отображения информации, характерной для данных приложений. Пример такого узла – **Internet Exp1orer 5.**

С помощью меню **Вид** можно переключаться между двумя режимами вывода информации: **Основные** (Basic) и **Дополнительно** (Advanced). В режиме **Дополнительно** отображается вся информация, доступная в режиме **Основные,** а также дополнительная информация, которая может представлять интерес для опытных пользователей или для специалистов службы поддержки Microsoft Technical Support.

Для поиска необходимых данных:

1. В меню **Действие** выберите команду **Поиск** (Find).
2. В окне **Найти** (Find What) введите слово или слова, соответствующие системной информации, которую вы ищете.
3. Установите необходимые опции поиска.
4. Для поиска только в узле определенной категории (например, Ресурсы или Компоненты) и во всех его подкатегориях установите флажок **Ограничить поиск внутри категории** (Restrict Search to Selected Category). Если снять данный флажок, поиск запускается в корневом узле.
5. Для поиска только имен узлов и подузлов дерева консоли, игнорируя любые совпадения в панели результатов, установите флажок **Искать только в категориях** (Search Categories Only). Снятие данного флажка запускает поиск в панели структуры и в панели результатов.
6. Для поиска информации по всем узлам и подузлам снимите оба флажка.
7. Нажмите кнопку **Найти далее**.

Для сохранения системных данных в файле системной информации выполните следующее:

1. В меню **Действие** выберите команду **Сохранить как файл сведений о системе** (Save As System Information File).
2. В поле **Папка** (Save in*)* задайте место сохранения файла.
3. В поле **Имя файла** (File name) введите имя файла.

4. В списке **Тип файла** (Save as type) выберите **Файл сведений о системе** (System Info File) и затем нажмите кнопку **Сохранить** (Save).

Файл будет сохранен как документ MSInfo. Для того чтобы открыть файл, дважды щелкните на его названии или выберите команду **Открыть** (Open) из контекстного меню. Файл будет открыт в отдельном окне **Сведения о системе**.

Оповещения и журналы производительности (Performance Logs and Alerts)

Оснастка расширения **Оповещения и журналы производительности** позволяет сконфигурировать журналы для записи данных и службу системных оповещений (Alerter) для уведомления о превышении каким-либо счетчиком определенного значения. Данная оснастка позволяет фиксировать данные о степени использования компьютера и работе служб (сервисов) на локальных и удаленных компьютерах.

Общие папки (Shared Folders)

Оснастка **Общие папки** позволяет просматривать информацию о соединениях и использовании ресурсов локального и удаленного компьютеров. Данная оснастка используется вместо программы Server в Control Panel системы Windows NT 4.0.

С помощью оснастки можно выполнять следующие задачи:

- Создавать, просматривать, изменять свойства и удалять общие ресурсы на локальном или удаленном компьютерах (Windows NT 4.0 или Windows 2000) и устанавливать разрешения на доступ к ним. Кроме того, можно управлять режимом кэширования общих папок (в случае их использования в качестве изолированных папок).
- Просматривать список удаленных пользователей, подключенных к компьютеру, и отключать их.
- Просматривать список файлов, открытых удаленными пользователями, и закрывать открытые файлы.

Оснастка **Общие папки** содержит три узла: **Ресурсы** (Shares), **Сеансы** (Sessions) и **Открытые файлы** (Open Files). При выборе данных узлов в панели результатов отображается содержание соответствующего узла.

Диспетчер устройств (Device Manager)

Узел **Диспетчер устройств** представляет одноименную оснастку, которая отображает в виде дерева все аппаратные устройства, установленные на локальном компьютере, и показывает их состояние, версии программных драйверов, используемые ресурсы (порты ввода/вывода, адреса памяти и IRQ). Данная оснастка позволяет изменять конфигурацию аппаратных элементов, а также механизм их взаимодействия с центральным процессором компьютера. Диспетчер устройств позволяет:

- Выяснить, корректно ли работает аппаратное обеспечение компьютера
- Изменить конфигурационные настройки оборудования
- Идентифицировать драйверы устройств, которые загружены для каждого устройства, и получить информацию о драйверах всех устройств
- Изменить дополнительные установки и параметры устройств
- Инсталлировать обновленные драйверы устройств
- Отключать и активизировать устройства
- Идентифицировать конфликты устройств и вручную конфигурировать установки ресурсов
- Распечатать суммарную информацию об устройствах, которые установлены на вашем компьютере

Оснастка **Диспетчер устройств** преимущественно используется для проверки состояния аппаратного обеспечения и обновления драйверов устройств на компьютере. Опытные пользователи, которые хорошо разбираются в аппаратном обеспечении компьютера, могут при помощи диагностических возможностей Диспетчера устройств устранять конфликты устройств и изменять установки ресурсов.

Изменение установок ресурсов может привести к отключению аппаратных компонентов и вызвать нарушение работы компьютера. Поэтому изменять установки ресурсов рекомендуется только пользователям, которые располагают достаточными знаниями об аппаратном обеспечении и аппаратных конфигурациях компьютеров. Как правило, пользователям нет необходимости изменять установки ресурсов, поскольку система Windows 2000 автоматически выделяет ресурсы аппаратным компонентам в ходе установки.

Диспетчер устройств можно использовать для управления устройствами только на локальном компьютере. На удаленном компьютере данная оснастка будет работать только в режиме просмотра.

Для каждого устройства на компьютере выделяется уникальный набор системных ресурсов для обеспечения корректной работы устройства. В число этих ресурсов входят:

- номера запросов на прерывание (Interrupt Request, IRQ);
- каналы прямого доступа к памяти (Direct Memory Access, DMA);
- адреса портов ввода/вывода (Input/output, I/O);
- диапазоны адресов памяти.

Механизм Plug and Play системы Windows 2000 производит выделение данных ресурсов автоматически в ходе установки всех устройств, которые поддерживают данный механизм. Если два устройства обращаются к одним ресурсам, то возникает аппаратный конфликт. В этом случае необходимо вручную изменить установки ресурсов для обеспечения их уникальности для каждого устройства. В обшем случае не следует изменять установки ресурсов вручную, поскольку при этом могут возникать сложные конфликтные ситуации, для устранения которых требуется глубокое понимание работы аппаратных и программных средств (в том числе – и драйверов).

Диспетчер устройств позволяет отключать и удалять устройства из системной конфигурации компьютера. При отключении устройства физическое устройство остается подключенным к компьютеру, но производятся соответствующие изменения в системном реестре, так что драйверы устройства не будут загружены при следующем запуске системы. Отключение устройств полезно, если необходимо иметь несколько аппаратных конфигураций компьютера или если работа ведется на портативном компьютере, используемом вместе со *станцией расширения* (док-станция, docking station).

Аппаратный профиль представляет собой набор инструкций, которые указывают системе Windows 2000, какие устройства следует запустить при включении компьютера. При инсталляции Windows 2000 создается аппаратный профиль по умолчанию. В данном профиле активизируются все устройства, имеющиеся на компьютере к моменту инсталляции операционной системы.

Аппаратные профили особенно полезны, если используется портативный компьютер. Например, можно создать профиль, который будет активизировать сетевую карту и внешний монитор, если компьютер

подключен к станции расширения, и профиль без поддержки данных устройств в противном случае.

Для создания нового аппаратного профиля откройте окно **Система** на панели управления и перейдите на вкладку **Оборудование** (Hardware). При наличии нескольких аппаратных профилей можно выбрать профиль по умолчанию, который будет загружаться при каждом запуске компьютера. После создания аппаратного профиля с помощью оснастки **Диспетчер устройств** можно активизировать и отключать устройства, которые содержит профиль.

Для изменения содержания панели результатов оснастки Диспетчер устройств выберите в меню **Вид** команду отображения **Устройства по типу/Устройства по подключению** (Devices by type/Devices by connection) или **Ресурсы по типу/Ресурсы по подключению** (Resources by type / Resources by connection). Устройства и ресурсы можно сортировать по типу (by type) или по подключению (by connection).

Примечание. Данное меню можно также открыть, щелкнув правой кнопкой мыши на узле Диспетчер устройств и выбрав команду **Вид** контекстного меню.

Для того чтобы просмотреть скрытые устройства, выберите пункт **Показать скрытые устройства** (Show hidden devices) в меню **Вид**. В число скрытых устройств входят устройства, не поддерживающие механизм Plug and Play (устройства с унаследованными драйверами прежних версий системы Windows NT), и устройства, которые были физически удалены из компьютера, но их драйверы остались.

Для того чтобы установить новое устройство, выберите в меню **Действие** команду **Обновить конфигурацию оборудования** (Scan for hardware changes). Оснастка проверит аппаратную конфигурацию компьютера и, если будут обнаружены новые устройства, запустит мастер установки новых устройств. Если потребовалось удалить некоторое устройство, выберите в меню **Действие** команду **Удалить** (Uninstall).

Окно свойств устройства можно открыть с помощью команды **Свойства** в меню **Действие.**

Локальные пользователи и группы (Local Users and Groups)

Узел Локальные пользователи и группы соответствует одноименной оснастке, аналогом которой в Windows NT Workstation 4.0 была административная утилита Диспетчер пользователей (User Manager). Функции и назначение остались неизменными: с помощью данной

оснастки создаются, модифицируются и удаляются учетные записи пользователей и групп на локальном компьютере. Использование этой оснастки будет описано позднее.

Запоминающие устройства

- Контейнер **Запоминающие устройства** содержит оснастки, которые используются для управления и обслуживания логическими дисками и дисковыми накопителями.
- Оснастка **Управление дисками** управляет логическими дисками. Эта оснастка будет описана далее.
- Оснастка **Дефрагментация диска** используется для анализа и дефрагментации удаленных и локальных логических дисков.
- Оснастка **Логические диски** представляет собой инструмент Windows Management Instrumentation (WMI), который позволяет управлять удаленными или локальными логическими дисками. С помощью оснастки можно
    - просматривать свойства дисков, такие как тип диска, его метку, тип файловой системы, объем используемого пространства;
    - менять метки (имена) дисков;
    - изменять параметры безопасности для дисков (только для томов с NTFS!): разрешения на доступ, политику аудита и владельца диска.
- С помощью оснастки **Съемные ЗУ** можно легко управлять библиотеками ленточных накопителей, сменными оптическими дисками и устройствами с автоматической подачей дисков (jukebox).

Службы и приложения (Services and Applications)

С помощью узла **Службы и приложения** можно, изменяя параметры, управлять инсталлированными службами или серверными приложениями, например, службами телефонии или сервером DHCP (это службы системы Windows 2000 Server). Такие службы и приложения могут работать не только в системе Windows 2000 Server, но и в Windows 2000 Professional (например, служба индексации).

Управляющий элемент WMI (WMI Control)

Узел **Управляющий элемент WMI** (и одноименная оснастка) позволяет конфигурировать средства (инструменты) Windows Management Instrumentation) в локальной системе и на удаленных компьютерах.

Службы (Services)

Тот, кто работал с предыдущимим версиями Windows NT, знает, что в Панели управления имелось приложение Службы (Services). с его помощью можно было просмотреть все службы, установленные в системе, узнать их статус, определить учетную запись, от имени которой они запускались, и порядок запуска. Это приложение по сути является инструментом администратора, и вынос его в Панель управления не вполне обоснован. В Windows 2000 это приложение реализовано в виде

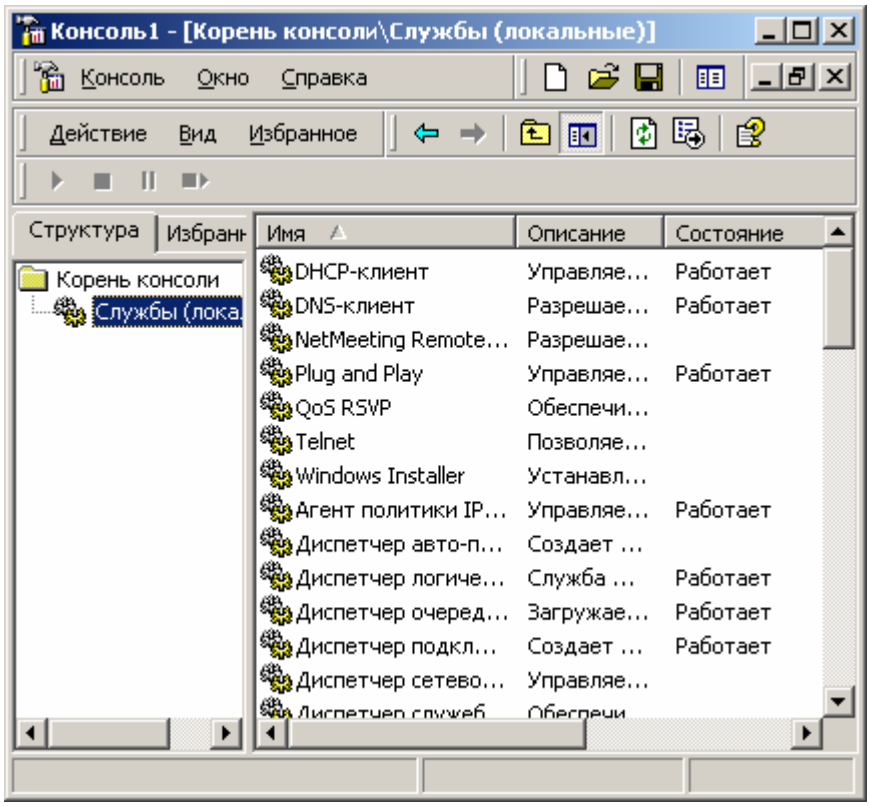

Рис. 11. Окно оснастки **Службы** на локальном компьютере

оснастки MMC и предоставляет ряд дополнительных возможностей. Вы можете запустить этот инструмен в виде изолированной оснастки или найти его в составе оснастки **Управление компьютером**.

В правой части изолированной оснастки **Службы** (рис. 11) появляется список установленных служб.

Если выбрать (дважды щелкнуть мышью) одну из служб в правом окне, оявится окно с вкладками свойства службы.

На вкладке **Общие** (рис. 12) приведены общие параметры служб:

- имя службы – используется для запуска службы и не может быть из-

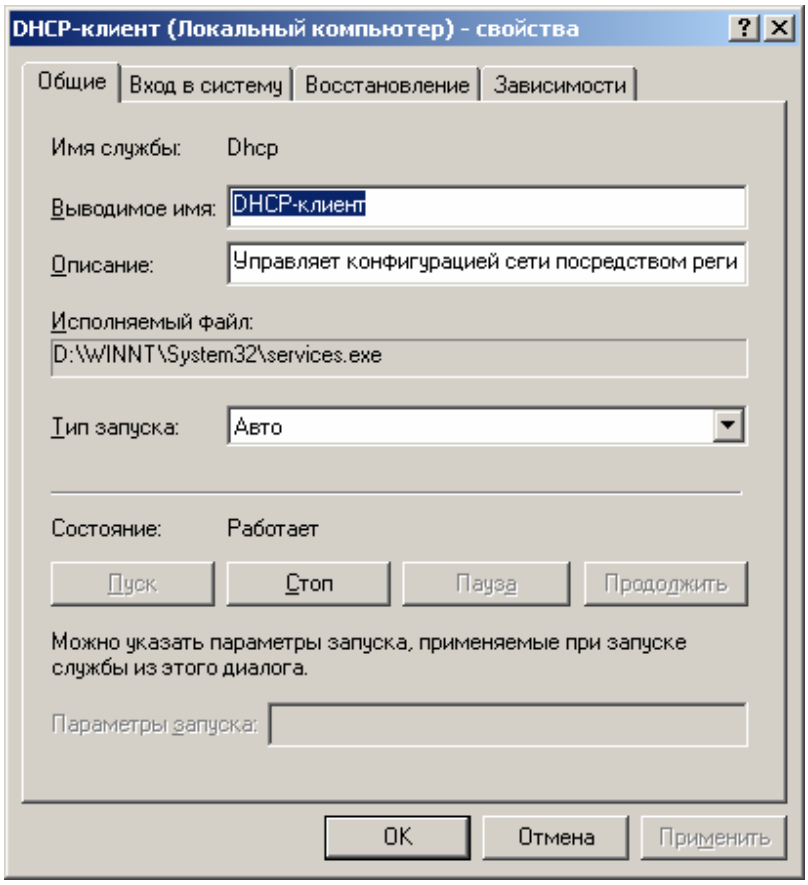

Рис.12. Окно свойств службы с вкладкой **Общие**

менено;

- выводимое имя – имя, появляющееся в списке служб, его вы можете изменять;
- описание – кратко поясняет назначение службы;
- путь к файлу – источнику службы: один файл может быть источником многих служб;
- тип запуска – в раскрывающемся списке вы можете указать, как служба будет запускаться (возможные значения: Авто, Вручную, Отключено);
- состояние – раздел текущего состояния содержит 4 кнопки (Пуск, Стоп, Пауза, Продолжить).

На вкладке **Вход в систему** вы можете сделать следующее:

- Указать учетную запись, от имени которой служба будет исполняться. При этом можно запускать ее от имени системы (с системной учетной записью), либо от имени учетной записи пользователя (для которой не установлена привилегия **Отказать во входе в качестве учетной записи**), указав ее пароль.
- Выбрать аппаратный профиль, в котором будет запрещено или разрешено исполнение службы.

На вкладке **Восстановление** вы можете указать системе, как поступить, если служба почему-либо не запустилась или ее исполнение прервалось.

Можно использовать до 3 попыток восстановления работы службы и для каждой из попыток указать выполняемое действие:

- ничего не делать;
- перезапуск службы;
- выполнение программы (в отдельном поле указывается путь к исполняемому файлу);
- перезапуск компьютера.

Последняя вкладка – **Зависимости.** Здесь наглядно показывается, какие службы влияют на работу рассматриваемой службы и какие зависят от нее. Вы можете просматривать, но не изменять зависимости. Эта информация чрезвычайно полезна, например, при выяснении, почему служба не запускается или сообщает об ошибках.

Служба индексирования (Indexing Service)

Служба индексирования инсталлируется как стандартный компонент Windows 2000. Эта служба индексирует содержимое всех дисков локального компьютера, что позволяет пользователю производить поиск любого слова или фразы, которые содержатся в документах на данном компьютере. Оснастка **Служба индексирования -** это новый инструмент с графической оболочкой для службы индексирования, который упрощает выполнение ряда административных задач, включая следующие:

- проверка состояния процесса индексации и параметров индексируемых каталогов;
- установка глобальных параметров для всех каталогов на компьютере;
- создание и конфигурирование новых каталогов для обеспечения оптимальной производительности;
- выбор индексируемых каталогов.

9. РАБОТА С ДИСКАМИ И ТОМАМИ

Данный раздел содержит сведения об организации дисковых систем, управлении ими с помощью оснастки **Управление дисками** (Disk Management) и оптимизации их работы. Средства этой оснастки позволяют работать с отказоустойчивыми системами, такими как зеркальные и чередующиеся тома с четностью (тома RAID 5).

*Оснастка **Управление дисками** (Disk Management)*

Оснастка **Управление дисками**, заменившая в Windows 2000 программу **Администратор дисков** (Disk Administrator), позволяет управлять дисковыми системами хранения данных. Для ее запуска необходимо обладать правами администратора.

Оснастка **Управление дисками** обладает следующими средствами:

- *Поддержка разделов и логических дисков Windows NT 4.0 и томов дисковых систем Windows 2000*. Применяя подход, предполагающий создание томов, вы избавитесь от ограничений, связанных с количеством основных разделов на одном диске (равное 4).
- *Управление дисковой системой в реальном времени*. Административные функции могут быть выполнены без отключения сервера и пре-

рывания работы пользователя. Например, вы можете создать, расширить том или установить его зеркальное отображение без перезагрузки системы. Большинство выполняемых при конфигурации дисковой системы изменений начинает действовать незамедлительно.

- *Удаленное и локальное управление дисковой системой.* Вы можете управлять любым удаленным компьютером, на котором работает Windows NT 4.0 или Windows 2000, где вы являетесь администратором.
- *Понятный и простой в работе интерфейс пользователя. С* помощью контекстных меню вы всегда можете узнать, какие задачи решаются с помощью оснастки в отношении некоторого объекта.

В отличие от предыдущих операционных систем производства компании Microsoft, позволяющих создавать только устройства с *базовым* режимом хранения информации (basic storage), Windows 2000 позволяет работать с новым типом устройств - устройствами с *динамическим* режимом хранения данных (dynamic storage). Диск, инициализированный для динамического хранения, называется *динамическим диском.* На нем могут находиться простые, составные, чередующиеся, зеркальные тома и тома RAID-5. Используя динамическое хранение, вы можете управлять дисками и томами без перезагрузки операционной системы. Дисковая система Windows 2000 может состоять из любой комбинации базовых и динамических дисков. Однако том, состоящий из нескольких дисков, должен иметь один режим хранения данных.

Работая при помощи оснастки **Управление дисками** с динамическими дисками, можно выполнять следующие функции:

- создавать и удалять простые (simple), составные (spanned), чередующиеся (stripped), зеркальные (mirrored) тома, а также тома RAID-5 (RAID-5 volume*);*
- форматировать тома для файловой системы FAT или NTFS;
- расширять том на дополнительные диски;
- восстанавливать зеркальные тома и тома RAID-5;
- повторно инициализировать отключенный диск;
- изменять динамический режим хранения на базовый.

Работая с помощью оснастки **Управление дисками** с базовыми томами, можно выполнять следующие функции:

- создавать и удалять основной (primary) и дополнительный (extended) разделы;
- создавать и удалять логические устройства внутри дополнительного раздела;
- форматировать разделы, присваивать им метки, а также помечать разделы как активные;
- инициализировать диски;
- уничтожать наборы томов, чередующиеся и зеркальные наборы и чередующиеся наборы с четностью;
- отключать зеркальный диск;
- восстанавливать зеркальный набор;
- восстанавливать чередующиеся наборы с четностью;
- изменять базовый режим хранения на динамический.

Таким образом, работая с оснасткой **Управление дисками,** можно использовать ее средства, ориентированные на управление динамическими томами, и одновременно осуществлять поддержку и управление базовыми дисками, созданными до появления Windows 2000. Для базовых дисков не поддерживаются следующие функции:

- создание наборов томов, чередующихся и зеркальных наборов и чередующихся наборов с четностью;
- расширение томов и наборов томов.

Для базовых и динамических дисков можно:

- контролировать информацию о дисках, такую как объем, доступное свободное пространство и текущий статус;
- просматривать свойства томов и разделов;
- устанавливать и изменять назначение имен томам жестких дисков или разделам, а также устройствам CD-ROM;

- устанавливать и проверять назначения общего доступа к тому или разделу.

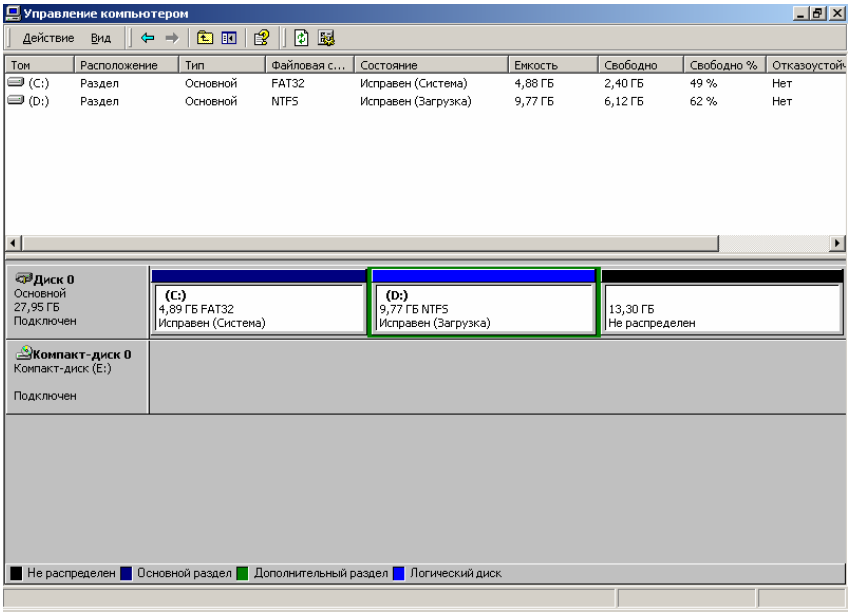

Рис. 13. Пример окна оснастки «Управление дисками»

Оснастку **Управление дисками** можно использовать как самостоятельно, так и в составе основного инструмента администрирования Windows 2000 – оснастки **Управление компьютером** (Computer Management). В первом случае при подключении оснастки к консоли управления можно в окне диалога **Выбор компьютера** (Choose Target Machine) выбрать положение переключателя **Локальный компьютер** (Local Computer), если вы хотите управлять локальным компьютером, либо положение **Другой компьютер** (Another Computer), если вы хотите управлять другим компьютером сети. В последнем случае в окне ввода следует указать имя компьютера (либо найти его, нажав кнопку **Обзор** (Browse)).

Пример окна оснастки **Управление дисками** приведен на рис. 13.

Базовый режим хранения информации

Понятие *раздела* обсуждалось ранее в курсе. Описывались основной и дополнительный раэделы. Эти понятия остаются такими же для базового режима хранения информации.

Динамический диск подразделяется на тома, а не на разделы. Том состоит из одного или нескольких физических дисков в одной из следующих конфигураций: простой том, составной том, зеркальный том, чередующийся том и том RAID-5.

Базовый диск может быть превращен в динамический диск в любое время. В табл. 2 показано соотношение между базовым и динамическим дисками.

Соотношение между базовыми и динамическими дисками

Таблица 2

Организация базового диска	Организация динамического диска
Системный и загрузочный разделы	Системный и загрузочный том
Основной раздел	Простой том
Дополнительный раздел	Простые тома и свободное пространство диска
Логическое устройство	Простой том
Набор томов	Составной том
Чередующийся набор	Чередующийся том
Зеркальный набор	Зеркальный том
Чередующийся набор с четностью	Том RAID-5

Динамический режим хранения информации

Том – это единица хранения, состоящая из свободного пространства на одном или нескольких дисках. Он может быть

отформатирован средствами файловой системы с присвоением ему имени. Тома на динамических дисках могут иметь одну из нескольких структур: простой, составной, зеркальный, чередующийся том и том RAID-5.

Простой том использует пространство одного диска. Это может быть один участок на диске или несколько участков, соединенных друг с другом. Простой том может быть расширен в пределах одного диска или на дополнительный диск. Если простой том распространен на несколько дисков, он становится составным томом. Простой том не обеспечивает отказоустойчивости.

Составной том состоит из связанного вместе пространства нескольких дисков (до 32 дисков). Он может быть распространен на дополнительные диски и не может принимать участие в зеркальных системах. Составные тома создаются, когда ни на одном жестком диске нет достаточного свободного пространства. Кроме того, создавая составные тома, можно распределять нагрузку на дисковые системы. Составные тома не обеспечивают отказоустойчивости. Поскольку тома такого типа расположены на нескольких жестких дисках, возрастает вероятность их отказа, связанного с выходом из строя одного из дисков.

Зеркальный том – это средство обеспечения отказоустойчивости, где данные дублируются на двух физических дисках. Все данные одного диска копируются на дополнительный диск, что обеспечивает возможность получения избыточности данных. Если один из дисков отказывает, данные могут быть доступны на уцелевшем диске зеркала. Зеркальный том не может быть расширен. Зеркало также известно как RAID-1.

Данные на *чередующемся томе* разбиваются при записи и помещаются на несколько физических дисков, причем информация равномерно распределяется среди всех дисков, входящих в состав такого тома. Такой подход удобен при необходимости быстрой записи или считывании с физических дисков большого объема информации. Скорость работы с дисковой системой увеличивается за счет распараллеливания потоков данных и одновременной записи или считывания информации с дисков тома. «Расщепление» информации также полезно при балансировке нагрузки ввода/вывода в многопользовательских приложениях. Тома с чередованием записываемой информации не обеспечивают отказоустойчивость. Том такого типа не может входить в зеркальный набор и его нельзя расширить. Чередование данных известно как RAID-0.

Том RAID-5 является средством обеспечения отказоустойчивости дисковой системы, поскольку данные тома расщепляются при записи на

три или большее количество дисков. Как уже обсуждалось, том *RAID-5* обеспечивает избыточность информации, подсчитывая контрольную сумму информации, расположенной на каждом диске. Контрольная сумма (вычисляемая величина, которая может быть использована для восстановления данных в случае их разрушения) также расщепляется и записывается на все диски массива. Если отказывает один из дисков массива, то информация, которая на нем находилась, может быть восстановлена с использованием данных работоспособных дисков и контрольной суммы. Том *RAID-5* не может входить в зеркальный набор и его нельзя расширить.

Свободное пространство – это неиспользованная и неформатированная часть жесткого диска, которая может быть использована при создании томов.

Системный том содержит файлы, жестко привязанные к оборудованию (Ntldr, Osloader.ex*e*, Boot.ini, Ntdetect.com), необходимые для загрузки Windows 2000.

Загрузочный том содержит файлы операционной системы Windows 2000, расположенные в папках *%SystemRoot%* и *%SystemRoot%\System32*.

Инициализация диска

После присоединения к компьютеру диск необходимо инициализировать. Только после этого на нем можно создавать тома и разделы. Если вы хотите создать простой том или планируете ввести новый диск в состав тома другого типа, нужно выбрать динамический режим хранения. Базовый режим хранения следует выбирать, если необходимо работать с разделами или логическими дисками (в том случае, когда на компьютере помимо Windows 2000 установлены другие системы – например, MS-DOS, – которые могут работать только с базовым режимом хранения данных).

Для инициализации диска:

1. Запустите оснастку **Управление дисками**.
2. В меню **Действие** (Action) выберите команду **Повторить сканирование дисков** (Rescan Disks).

Новые диски, присоединенные к компьютеру, подключаются как базовые. Впоследствии базовые диски могут быть превращены в динамические:

- Укажите нужный базовый диск и нажмите правую кнопку мыши. В появившемся контекстном меню выберите команду **Обновление** до **динамического диска** (Upgrade to Dynamic Disk).

Возможно и обратное превращение. Однако динамические тома нельзя непосредственно конвертировать в разделы: предварительно все тома на диске придется удалить. Чтобы превратить динамический диск в базовый:

- Укажите динамический диск и нажмите правую кнопку мыши. В появившемся контекстном меню выберите команду **Возвратить к базовому диску** (Revert to Basic Disk).

Управление динамическими дисками

В динамическом режиме хранения информация располагается на томах, которые несовместимы с разделами дисков, созданными в Windows NT 4.0. Для конфигурирования дискового пространства при обновлении Windows NT следует использовать программу Setup. Кроме того, если вы устанавливаете Windows 2000 на существующий диск и собираетесь создавать на нем новые тома или логические устройства, необходимо предварительно создать архивную копию данных, находящихся на диске.

Работа с томами

С помощью средств Windows 2000 можно весьма гибко управлять дисковой системой. Вы можете создать набор томов на свободном пространстве физических жестких дисков. Кроме того, созданные вами тома могут включать в себя несколько дисков и входить составной частью в систему обеспечения отказоустойчивости системы хранения данных.

Каждый том диска может иметь одну из двух файловых систем – FAT (FAT16 или FAT32) или NTFS. Если вы хотите работать с несколькими файловыми системами, а на вашем жестком диске есть только один том, на том же диске вам придется создать второй том. Если же на диске не осталось свободного пространства, следует заново установить Windows 2000 таким образом, чтобы оставить свободное пространство, позволяющее создать необходимое количество томов.

Если вы работаете только с операционной системой Windows 2000, один том может занимать весь жесткий диск. Однако, если планируется использование других операционных систем, это следует учитывать при разбивке дискового пространства и соответственно указать размер тома, на котором будет установлена операционная система

Windows NT 2000. После завершения установки с помощью оснастки **Управление дисками** на оставшемся свободном дисковом пространстве можно создать дополнительные тома. Например, если вы будете устанавливать на жестком диске другую операционную систему - MS-DOS или UNIX, имеющую несовместимую с Windows 2000 файловую систему, следует создать второй том. Необходимо отметить, что MS-DOS и Windows 2000 могут существовать на одном и том же томе, если он сформатирован для FAT.

Для разбивки дискового пространства до установки Windows 2000 можно использовать программы Fdisk (для FAT) и другие утилиты (для NTFS). Следует помнить, что Fdisk «не видит» тома, сформатированные для NTFS.

Все изменения, сделанные на диске, немедленно вступают в силу. Поэтому не нужно сохранять их или перезагружать систему.

Установка нового динамического диска

Динамическим диском называется физический диск, на котором с помощью оснастки **Управление дисками** созданы динамические тома. На свободном пространстве динамического диска можно создать следующие тома:

- системный и загрузочный том;
- дополнительный простой том;
- другие типы томов Windows 2000: составные, чередующиеся, зеркальные или RAID-5 (предполагается, что в системе установлено несколько жестких дисков).

Создание простого тома

Простые тома могут быть созданы только на динамических дисках. Они не могут содержать разделы или логические диски. Доступ к таким томам возможен только из Windows 2000. Создание простого тома выполняется с помощью мастера создания тома (Create Volume Wizard) оснастки **Управление дисками.**

Расширение простых и составных томов

Простой том может быть расширен за счет других областей диска. При расширении простого тома на другой диск он становится составным томом. После того как простой том становится составным томом, он может подвергаться дальнейшим расширениям, захватывая все больше

свободного пространства на жестких дисках, установленных в системе. Однако следует отметить, что ни одна часть составного тома не может быть уничтожена отдельно от остальных его частей. Составные тома не могут принимать участие в зеркале и записи данных с чередованием.

Назначение имен устройствам

Операционная система Windows 2000 позволяет создать более 24 томов. Однако вы можете присвоить томам только 24 имени (буквы алфавита). Буквы A и B зарезервированы для флоппи-дисководов. (Если на компьютере нет второго флоппи-дисковода, можно использовать букву B для сетевого устройства.)

Windows 2000 допускает статическое именование устройств. Это значит, что определенные имена могут быть назначены конкретным жестким дискам и томам на постоянной основе. Если в существующую систему компьютера устанавливается новый жесткий диск, назначение его имени не влияет на имена остальных устройств.

Форматирование динамических томов и установка их меток

Перед тем как сохранять файлы в папках, созданных на томе, необходимо его отформатировать для определенной файловой системы. В процессе форматирования можно указать информативную метку тома. Если на томе установлена NTFS, можно использовать сжатие данных.

Для форматирования тома в Проводнике или в оснастке **Управление дисками** укажите том и нажмите правую кнопку мыши. В открывшемся контекстном меню выберите команду **Форматировать** (Format).

Удаление динамических томов

Перед удалением тома в Windows 2000 необходимо убедиться, что расположенная на нем ценная информация скопирована в другое место и целостность скопированных данных проверена.

Операционная система Windows 2000 налагает определенные требования на операцию удаления томов. Нельзя удалить том, содержащий системные файлы (системный том). Нельзя удалить индивидуальные тома, являющиеся частью набора томов, без удаления всего набора.

Для удаления тома с помощью оснастки **Управление дисками** укажите его и нажмите правую кнопку мыши. В появившемся контекстном меню выберите команду **Удалить том** (Delete Volume).

Режим базового хранения данных используется при организации диска, принятой в Windows NT 4.0 и связанной с созданием разделов. В процессе обновления (upgrade) системы уже разбитые диски автоматически инициализируются как базовые диски, что обеспечивает обратную совместимость. Новые или пустые диски могут быть инициализированы как базовые или динамические.

С помощью оснастки **Управление дисками** можно поддерживать разделы и тома, созданные в Windows NT 4.0, однако, несмотря на то, что вы можете создавать или удалять разделы, нельзя создать новый зеркальный или чередующийся набор. Для создания новой отказоустойчивой дисковой системы следует создавать тома на динамических дисках.

Работа с разделами

В Windows 2000 вы можете работать с разделами базового диска точно так же, как это делалось в Windows NT 4.0, с одним исключением: больше не нужно явно сохранять сделанные изменения или перезагружать компьютер для их активизации. На одном физическом диске может быть создано до четырех разделов. Один из них может быть дополнительным разделом, на котором может быть создано несколько логических дисков. Пространство дополнительного раздела не может быть использовано для организации наборов томов или других типов отказоустойчивых томов.

Изменения, сделанные с помощью оснастки **Управление дисками,** *сразу же вступают в силу.* Если сделанные изменения не касаются существующих на диске файлов, система отрабатывает изменения без запроса дополнительного подтверждения правильности выполняемого действия. Перед тем как вы получите возможность работать с созданными разделами, необходимо индивидуально отформатировать каждый раздел для определенной файловой системы. В процессе форматирования можно указать метку раздела.

В каждом разделе может быть установлена одна из двух файловых систем: FAT или NTFS. Если вы хотите работать с обеими файловыми системами, но на вашем жестком диске есть только один раздел, следует переустановить операционную систему Windows 2000 и разбить жесткий диск таким образом, чтобы на нем было несколько разделов.

Системный том Windows 2000 – это том, на котором находятся файлы, жестко связанные с оборудованием системы компьютера,

необходимые для загрузки Windows 2000. Системный том должен находиться в основном активном разделе. Кроме того, системный том должен находиться на жестком диске, доступ к которому компьютер получает сразу же после начала работы. В системе может быть только один активный раздел. Если вы хотите загружать другую операционную систему, следует пометить ее системный раздел как активный и перезагрузить компьютер.

Загрузочный том в Windows 2000 – это том (либо FAT, либо NTFS), содержащий файлы операционной системы Windows 2000. Загрузочный раздел может совпадать с системным разделом. Он может быть частью массива дисков или набора томов.

Перед удалением раздела или логического диска в Windows 2000 необходимо убедиться, что расположенная на них ценная информация скопирована в другое место, и целостность скопированных данных проверена.

Операционная система Windows 2000 налагает определенные требования на операцию удаления разделов: нельзя уничтожать системный раздел или удалять индивидуальные разделы, являющиеся частью набора, без уничтожения всего набора. Кроме того, Windows 2000 требует, чтобы все логические устройства и другие тома, находящиеся в дополнительном (extended) разделе, были уничтожены перед уничтожением самого дополнительного раздела.

Создание базовых разделов

Создать новый раздел можно только в том случае, если на жестком диске компьютера осталось свободное пространство.

Для создания базового раздела:

1. В окне оснастки **Управление дисками** щелкните на свободном пространстве диска (помеченном на экране как **Свободно** (Unallocated)).
2. В меню **Действие** выберите команду **Создать** (New). В появившемся меню выберите команду **Раздел** (Partition).
3. Откроется начальное окно Мастера создания раздела (Create Partition Wizard). Прочтите выведенный в нем текст и нажмите кнопку **Далее**.
4. В следующих окнах мастера вы можете сообщить тип раздела (основной (Primary) или дополнительный (Extended)), имя устройства и параметры форматирования.

5. Сообщив всю необходимую информацию, нажмите кнопку **Готово** (Finish) в последнем окне мастера. В результате будет создан новый раздел.

При создании раздел необходимо отформатировать. При форматировании может быть задано несколько файловых систем: FAT16, FAT32 или NTFS 5.0.

Создание и удаление набора томов и чередующихся наборов

Средства Windows 2000 не позволяют создать новые наборы базовых томов или чередующиеся наборы – вы можете только уничтожить их. Для того чтобы уничтожить набор томов, сначала создайте резервную копию всей информации, расположенной на дисках набора, поскольку она будет уничтожена вместе с набором. Затем уничтожьте набор томов.

Для создания нового составного тома, который является эквивалентом набора томов базового диска, или чередующегося тома – эквивалента чередующегося набора, следует использовать диск, инициализированный для динамического режима хранения. Для того чтобы конвертировать существующий набор томов, измените режим работы физических дисков, на которых находятся разделы, на динамический.

Обеспечение отказоустойчивости дисковых систем

Отказоустойчивые дисковые системы подразделяются на шесть уровней RAID от 0 до 5. Каждый уровень характеризуется определенным соотношением производительности системы с ее надежностью и стоимостью. Оснастка **Управление дисками** позволяет работать с системами RAID уровней 1 и 5.

Эти системы могут быть реализованы на уровне оборудования или на уровне программного обеспечения. Аппаратные решения предполагают, что созданием и восстановлением избыточной информации управляет контроллер дисковой системы. В операционной системе Windows 2000 эта задача может быть решена с помощью программного обеспечения. Аппаратурная реализация RAID обладает более высокой производительностью по сравнению с программным решением, реализация которого возможна в Windows 2000 Server.

10. ТИПОВЫЕ ЗАДАЧИ АДМИНИСТРИРОВАНИЯ

Создание локальных учетных записей пользователей и групп

Создание учетных записей пользователей и групп занимает важное место в обеспечении безопасности Windows 2000, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации, разрешить или запретить им выполнить в сети определенное действие, например, архивацию данных или завершение работы компьютера. Обычно право доступа ассоциируется с объектом – файлом или папкой. Оно определяет возможность данного пользователя получить доступ к объекту.

*Оснастка **Локальные пользователи и группы** (Local Users and Groups)*

Оснастка **Локальные пользователи и группы –** это инструмент

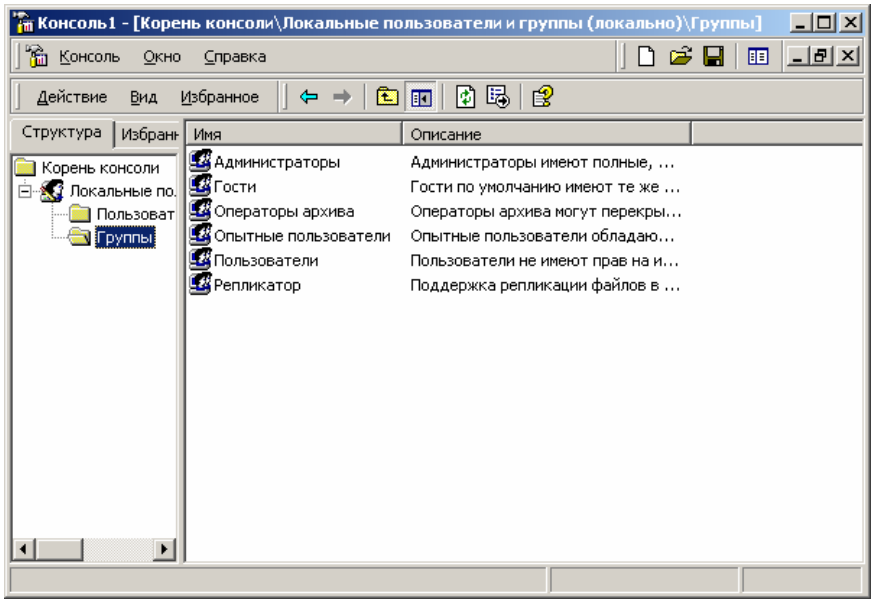

Рис. 14. Окно оснастки **Локальные пользователи и группы**

MMC, с помощью которого выполняется управление локальными учетными записями пользователей и групп – как на локальном, так и на удаленном компьютерах. С ним можно работать на рабочих станциях и автономных серверах Windows 2000, как на изолированных, так и рядовых членах домена. На контроллерах домена Windows 2000 инструмент **Локальные пользователи и группы** недоступен, поскольку все управление учетными записями и группами в домене выполняется с помощью оснастки **Пользователи и компьютеры Active Directory** (Active Directory Users and Computers). Запускать оснастку **Локальные пользователи и группы** может любой пользователь. Выполнять администрирование учетных записей могут только администраторы и члены группы Опытные пользователи (Power Users).

Окно изолированной оанаатки **Локальные пользователн и группы** выглядит аналогично показанному на рис. 14.

Папка Пользователи (Users)

Сразу после установки системы Windows 2000 (рабочей станции или сервера, являющегося членом домена) папка **Пользователи** содержит две встроенные учетные записи – Администратор (Administrator) и Гость (Guest). Они создаются автоматически при установке Windows 2000. Ниже даны описания свойств обеих встроенных учетных записей:

- **Администратор -** эту учетную запись используют при установке и настройке рабочей станции или сервера, являющегося членом домена. Она не может быть уничтожена, блокирована или удалена из группы Администраторы (Administrators), ее можно только переименовать.
- **Гость** – эта учетная запись применяется в компьютере без использования специально созданной учетной записи. Учетная запись Гость не требует ввода пароля и по умолчанию блокирована. (Обычно пользователь, учетная запись которого блокирована, но не удалена, при регистрации получает предупреждение и входить в систему не может). Она является членом группы Гости (Guests). Ей можно предоставить права доступа к ресурсам системы точно так же, как любой другой учетной записи.

Папка Группы (Groups)

После установки системы Windows 2000 (рабочей станции или сервера, являющегося членом домена) папка **Группы** (Groups) содержит шесть встроенных групп. Они создаются автоматически при установке Windows 2000. Ниже описаны свойства всех встроенных групп:

- **Администраторы** (Administrators) – ее члены обладают полным доступом ко всем ресурсам системы. Это единственная встроенная группа, автоматически предоставляющая своим членам весь набор встроенных прав.

- **Операторы архива** (Backup Operators) – члены этой группы могут архивировать и восстанавливать файлы в системе независимо от того, какими правами эти файлы защищены. Кроме того, операторы архива могут входить в систему и завершать ее работу, но они не имеют права изменять настройки безопасности.

- **Гости** (Guests) – эта группа позволяет выполнить регистрацию пользователя с помощью учетной записи *Гость* и получить ограниченные права на доступ к ресурсам системы. Члены этой группы могут завершать работу системы.

- **Опытные пользователи** (Power Users) – члены этой группы могут создавать учетные записи пользователей, но они имеют право модифицировать настройки безопасности только для созданных ими учетных записей. Кроме того, они могут создавать локальные группы и модифицировать состав членов созданных ими групп. То же самое они могут делать с группами Пользователи, Гости и Опытные пользователи. Члены группы Опытные пользователи не могут модифицировать членство в группах Администраторы и Операторы архива. Они не могут быть владельцами файлов, архивировать или восстанавливать каталоги, загружать и выгружать драйверы устройств и модифицировать настройки безопасности и журнал событий.

- **Репликатор** (Replicator) – членом группы Репликатор должна быть только учетная запись, с помощью которой можно зарегистрироваться в службе репликации контроллера домена. Ее членами не следует делать рабочие учетные записи.

- **Пользователи** (Users) – члены этой группы могут выполнять большинство пользовательских функций, например, запускать приложения, пользоваться локальным или сетевым принтером, завершать работу системы или блокировать рабочую станцию. Они также могут создавать локальные группы и регулировать состав их членов. Они не могут получить доступ к общему каталогу или создать локальный принтер.

В качестве примера использования оснастки **Локальные пользователи и группы** для работы с учетными записями рассмотрим процедуру создания пользовательской учетной записи.

Создание учетной записи

Для создания учетной записи:

1. В оснастке **Локальные пользователи и группы** установите указатель на папку Пользователи и нажмите правую кнопку. В контекстном меню выберите команду **Новый пользователь** (New User).

2. Появится окно диалога **Новый пользователь** (New User). В поле **Пользователь** (User Name) введите имя создаваемого пользователя. В поле **Полное имя** (Full name) введите полное имя создаваемого пользователя. В поле **Описание** (Description) введите описание создаваемого пользователя или его учетной записи. В поле **Пароль** (Password) введите пользователя и в поле **Подтверждение** (Confirm Password), подтвердите его правильность вторичным вводом. Длина пароля не может превышать 14 символов.

3. Установите или снимите флажки **Потребовать смену пароля при следующем входе в систему** (User must change password at next logon), **Запретить смену пароля пользователем** (User cannot change password), **Срок пароля не ограничен** (Password never expires) и **Отключить учетную запись** (Account is disabled).

4. Чтобы создать еще одного пользователя, нажмите кнопку **Создать** (Create) и повторите шаги с 1 по 3. Для завершения работы нажмите кнопку **Создать** и затем **Закрыть** (C1ose).

Имя пользователя должно быть уникальным для компьютера. Оно должно содержать до 20 символов верхнего и нижнего регистра. Ниже приведены символы, применение которых в имени пользователя недопустимо:

" / \ [ ] : ; | = , + * ? < >

Имя пользователя не может состоять целиком из точек и пробелов.

Изменение и удаление учетных записей

Изменять, переименовывать и удалять учетные записи можно с контекстного меню, вызываемого щелчком правой кнопки мыши на имени пользователя, либо – меню **Действие** (Action) на панели меню оснастки **Локальные пользователи и группы** (при этом в правом подокне оснастки должна быть выбрана модифицируемая или удаляемая учетная запись пользователя).

Поскольку переименованная учетная запись сохраняет *идентификатор безопасности (Security Identifier*т, SID), она сохраняет и все свои свойства, пример, описание, полное имя пароля, членство в группах и т.д.

Управление локальными группами

Создание локальной группы

Для создания локальной группы:

1. В окне оснастки **Локальные пользователи и группы** установите указатель мыши на папке **Группы** и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Новая группа** (New Group).
2. В поле **Имя группы** (Group Name) введите имя новой группы.
3. В поле **Описание** (Description) введите описание новой группы.
4. В поле **Члены группы** (Members) можно сразу же добавить пользователей и группы, которые войдут в данную группу: для этого нужно нажать кнопку **Добавить** (Add) и выбрать их в списке.
5. Для завершения нажмите кнопку **Создать** и затем **Закрыть**.

Имя локальной группы должно быть уникальным в пределах компьютера, может содержать до 256 символов в верхнем и нижнем регистрах. В имени группы запрещено применение символа обратного слэша (\).

Изменение членства в локальной группе

Чтобы добавить или удалить учетную запись пользователя из группы:

1. В окне оснастки **Локальные пользователи и группы** щелкните на папке **Группы**.

2. В правом подокне установите указатель мыши на модифицируемую группу и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Добавить в группу** (Add to group) или **Свойства** (Properties).

3. Для того чтобы добавить новые учетные записи в группу, нажмите кнопку Добавить. Далее следуйте указаниям окна диалога **Выбор: Пользователи или Группы** (Select Users or Groups).

4. Для того чтобы удалить из группы некоторых пользователей, в поле **Члены группы** окна свойств группы выберите одну или несколько учетных записей и нажмите кнопку **Удалить** (Remove).

В локальную группу можно добавлять как локальных пользователей, созданных на компьютере, так и пользователей и глобальные группы, созданные в домене, к которому принадлежит компьютер, или в доверяемых доменах.

Примечание. Встроенные группы не могут быть удалены. Удаленные группы не могут быть восстановлены. Удаление группы не отражается на входящих в нее пользователей.

Управление рабочей средой пользователя

Рабочая среда пользователя состоит из настроек рабочего стола, например, цвета экрана, настроек мыши, размера и расположения окон, из настроек процесса обмена информацией по сети и с устройством печати, переменных среды, параметров реестра и набора доступных приложений.

Для управления средой пользователя предназначены следующие средства Windows 2000:

- *Сценарий входа в сеть* (*сценарий регистрации)* представляет собой командный файл, имеющий расширение .bat, или исполняемый файл с расширением .exe, который выполняется при каждой регистрации пользователя в сети. Сценарий может содержать команды операционной системы, предназначенные, например, для создания соединения с сетью или для запуска приложения. Кроме того, с помощью сценария можно устанавливать значения переменных среды, указывающих пути поиска, каталоги для временных файлов и другую подобную информацию.

- *Профили пользователей.* В профиле пользователя хранятся все настройки рабочей среды компьютера, на котором работает Windows 2000, определенные самим пользователем. Это могут быть, например, настройки экрана и соединения с сетью.

- *Сервер сценариев Windows* (Windows Scripting Host, WSH). Сервер сценариев независим от языка и предназначен для работы на 32-разрядных платформах Windows. Он включает в себя как ядро сценариев Visual Basic Scripting Edition (VBScript), так и JScript. Сервер сценариев Windows предназначен для выполнения сценариев прямо на рабочем столе Windows или на консоли команд. При этом сценарии не надо встраивать в документ HTML.

Профили пользователей

На изолированном компьютере с Windows 2000 локальные профили пользователей создаются автоматически. Информация локальных профилей необходима для поддержки настроек рабочего стола локального компьютера, характерных для конкретного пользователя. Профиль создается для каждого пользователя в процессе его первой регистрации в компьютере. Профиль пользователя обладает следующими преимуществами:

- При регистрации пользователя в системе рабочий стол получает те же настройки, какие существовали в момент предыдущего выхода пользователя из системы.

- Несколько пользователей могут работать на одном и том же компьютере в индивидуальных средах.

- Профили пользователей могут быть сохранены на сервере. В этом случае пользователь получает возможность работать со своим профилем при регистрации на любом компьютере сети. Такие профили называются *перемещаемыми* (roaming profile).

Пользовательские профили можно применять следующим образом:

- Создать несколько типов профилей и назначить их определенным группам пользователей. Это позволит получить несколько типов рабочих сред, соответствующих различным задачам, решаемым пользователями.

- Назначать общие групповые настройки всем пользователям.

- Назначать обязательные профили, какие-либо настройки которых пользователи изменять не могут.

Итак, профили можно классифицировать:

- по месту использования:
  - локальные;
  - перемещаемые;
- по возможности изменения:
  - изменяемые;
  - обязательные;
- по числу использующих данный профиль пользователей:
  - групповой;
  - индивидуальный;
  - профиль по умолчанию (существует на каждом компьютере и при первой регистрации именно он устанавливается для пользователя, а затем в него вносятся все изменения, сделанные пользователем).

Настройки, хранящиеся в профиле пользователя

Профиль пользователя хранит настройки конфигурации и параметры, индивидуально назначаемые каждому пользователю и полностью определяющие его рабочую среду (табл. 3).

Настройки профиля пользователя

Таблица 3

Объект	Соответстующие ему параметры
Windows NT Explorer	Все настройки, определяемые самим пользователем, касающиеся программы Проводник (Windows NT Explorer)
Панель задач	Все персональные группы программ и их свойства, все программные объекты и их свойства, все настройки панели задач.
Настройки принтера	Сетевые соединения принтера

Панель управления	Все настройки, определенные самим пользователем, касающиеся панели управления.
Стандартные	Настройки всех стандартных приложений, запускаемых для конкретного пользователя
Приложения, работающие в ОС Windows NT 2000	Любое приложение, специально созданное для работы в среде Windows *2000,* может обладать средствами отслеживания своих настроек относительно каждого пользователя. Если такая информация существует, она хранится в профиле пользователя
Электронная подсказка	Любые закладки, установленные в справочной системе Windows 2000
Консоль управления Microsoft	Индивидуальный файл конфигурации и текущего состояния консоли управления

Структура профиля пользователя

Профиль пользователя представляет собой совокупность файлов и папок с определенными именами, которые нельзя изменять. Каждая папка содержит определенную группу настроек.

Профиль пользователя создается на основе профиля, назначаемого по умолчанию. Он хранится на каждом компьютере, где работает Windows 2000. Файл NTuser.dat, находящийся в папке Default User, содержит настройки конфигурации, хранящиеся в реестре Windows 2000. Кроме того, каждый профиль пользователя использует общие программные группы, находящиеся в папке **All Users**.

Папки профиля пользователя

Как уже говорилось, при создании профиля пользователя используется профиль, назначаемый по умолчанию, находящийся в папке **Default User.** Папка **Default User**, папки профилей индивидуальных пользователей, а также папка **All Users**, находятся в папке **Documents and Settings** корневого каталога. В папке **Default User** находятся файл Ntuser.dat и список ссылок на объекты рабочего стола. На рис. 15 показана структура папок локального профиля пользователя. В этих папках, в частности, хранятся ссылки на личные объекты рабочего стола.

В табл. **.4 перечислены подпапки, находящиеся внутри папки, профиля пользователя, и описано их содержимое.

Содержимое папки локального профиля пользователя

Таблица 4

Подпапка	Содержимое
Application Data	Данные, относящиеся к конкретному приложению, например, индивидуальный словарь. Разработчики приложений сами принимают решение, какие данные должны быть сохранены в папке профиля пользователя.
Cookies	Служебные файлы, получаемые с просматриваемых с веб-серверов
Local Settings	Данные о локальных настройках, влияющих на работу программного обеспечения компьютера
NetHood	Ярлыки объектов сетевого окружения
PrintHood	Ярлыки объектов папки принтера
Recent	Ярлыки недавно используемых объектов (например, недавно редактированных текстовых документов)
SendTo	Ярлыки объектов, куда могут посылаться документы (появляются в контекстном меню файла или папки при выборе опции Отправить)
Главное меню (Start Menu)	Ярлыки программ
Избранное (Favorites)	Ярлыки часто используемых программ и папок
Мои документы (My documents)	Данные о документах и графических файлах, используемых пользователем
Рабочий стол (Desktop)	Объекты рабочего стола, включая файлы и яр-

Подпапка	Содержимое
	лыки
Шаблоны (Templates)	Ярлыки шаблонов (например, программ из пакета Microsoft Office)

Папка All Users

Настройки, находящиеся в папке **All Users,** не копируются в папки профиля пользователя, но используются для его создания. Платформы Windows NT поддерживают два типа программных групп:

- **Общие программные группы.** Они всегда доступны на компьютере, независимо от того, кто зарегистрирован на нем в данный момент. Только администратор может добавлять объекты к этим группам, удалять или модифицировать их.
- **Персональные программные группы.** Они доступны только создавшему их пользователю.

Общие программные группы хранятся в папке **All Users**, находящейся в папке **Documents and Settings.** Папка **All Users** также содержит настройки для рабочего стола и меню **Пуск.** Группы этого типа на компьютерах, где работает Windows 2000, могут создавать только члены группы Администраторы.

Создание локального профиля пользователя

Локальный профиль пользователя хранится на компьютере в папке, имя которой совпадает с именем данного пользователя, находящейся в папке **Documents and Settings.** Если для данного пользователя не существует сконфигурированный перемещаемый (находящийся на сервере) профиль, то при первой регистрации пользователя в компьютере для него создается индивидуальный профиль. Содержимое папки **Default User** копируется в папку нового профиля пользователя. Информация профиля вместе с содержимым папки **All Users** используется при конфигурации рабочей среды пользователя. При завершении пользователем работы на компьютере все сделанные изменения настроек рабочей среды, выбираемых по умолчанию, записываются в его профиль. Содержимое папки **Default User** остается неизменным.

Если пользователь имеет отдельную учетную запись на локальном компьютере и в домене, для каждой из них создается свой

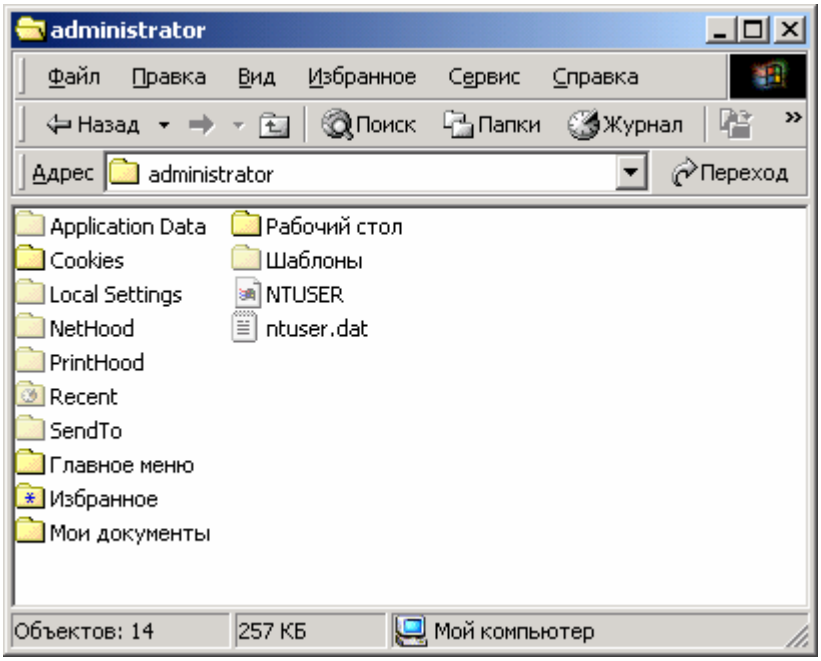

Рис. 15. Структура подпапок профиля пользователя

профиль пользователя, поскольку регистрация на компьютере происходит с помощью различных учетных записей. При завершении работы все сделанные изменения также записываются в соответствующий данной учетной записи профиль.

Папка профиля пользователя на локальном компьютере содержит файл NTuser.dat и файл журнала транзакций с именем NTuser.dat.LOG (рис. 15). Он нужен для обеспечения отказоустойчивости, позволяя Windows 2000 восстанавливать профиль пользователя в случае сбоя при модификации содержимого файла NTuser.dat .

Перемещаемые профили пользователя

Перемещаемые профили пользователя могут быть созданы тремя способами:

- Каждой учетной записи назначается путь к профилю пользователя. В этом случае на сервере происходит автоматическое создание пустой

папки профиля пользователя. Затем пользователь может сам создать свой профиль.

- Каждой учетной записи назначается путь к профилю пользователя. Затем в папку, указанную в пути, копируется приготовленный заранее профиль пользователя.
- Каждой учетной записи назначается путь к профилю пользователя. Затем в папку, указанную в пути, копируется приготовленный заранее профиль пользователя. После этого файл NTuser.dat, путь к которому указан в каждой учетной записи, переименовывается в NTuser.man. В этом случае создается обязательный профиль пользователя.

Примечание. В перемещаемый профиль не входит подпапка **Local Settings,** где, в частности, хранятся архивы программы Outlook Express, папки Temporary Internet Files и History и временные файлы!

Имя сервера (это может быть любой сервер в сети), на котором будут находиться перемещаемые профили пользователей, указывается с помощью оснастки **Локальные пользователи и группы** и вкладки **Профиль** (Profile) окна свойств пользователя. В результате при завершении работы пользователя на компьютере его профиль сохраняется как на локальном компьютере, так и в папке на сервере, в соответствии с путем профиля. При следующей регистрации пользователя в сети дата копии профиля, находящейся на сервере, сравнивается с копией, расположенной локально на компьютере. Если они отличаются, информация берется из более свежей копии. Перемещаемый профиль находится в централизованном хранилище профилей в масштабах домена. Он может быть доступен только при условии работоспособности хранящего его сервера. В обратном случае используется локальная кэшированная копия профиля пользователя. Если пользователь первый раз зарегистрировался в компьютере, создается новый профиль. В любом случае, если хранящийся централизованно профиль пользователя недоступен, он не обновляется при завершении работы. При следующей регистрации в компьютере пользователю придется напрямую указать копию профиля – более новую локальную или старую копию, находящуюся на сервере.

Примечание. Настройка перемещаемых профилей пользователей, являющихся членами домена Windows 2000, выполняется при помощи оснастки **Пользователи и компьютеры Active Directory** (Active Directory Users and Computers

Алгоритм создания перемещаемого профиля:

1. С помощью оснастки **Локальные пользователи и группы** можно указать имя сервера, где будет храниться заранее созданный перемещаемый профиль пользователя.

2. В окне **Система** (System), вызываемом из панели управления, перейдите на вкладку **Профили пользователей** (User Profiles), нажмите кнопку **Копировать** (Copy To) и скопируйте профиль заранее созданного пользователя на сервер.

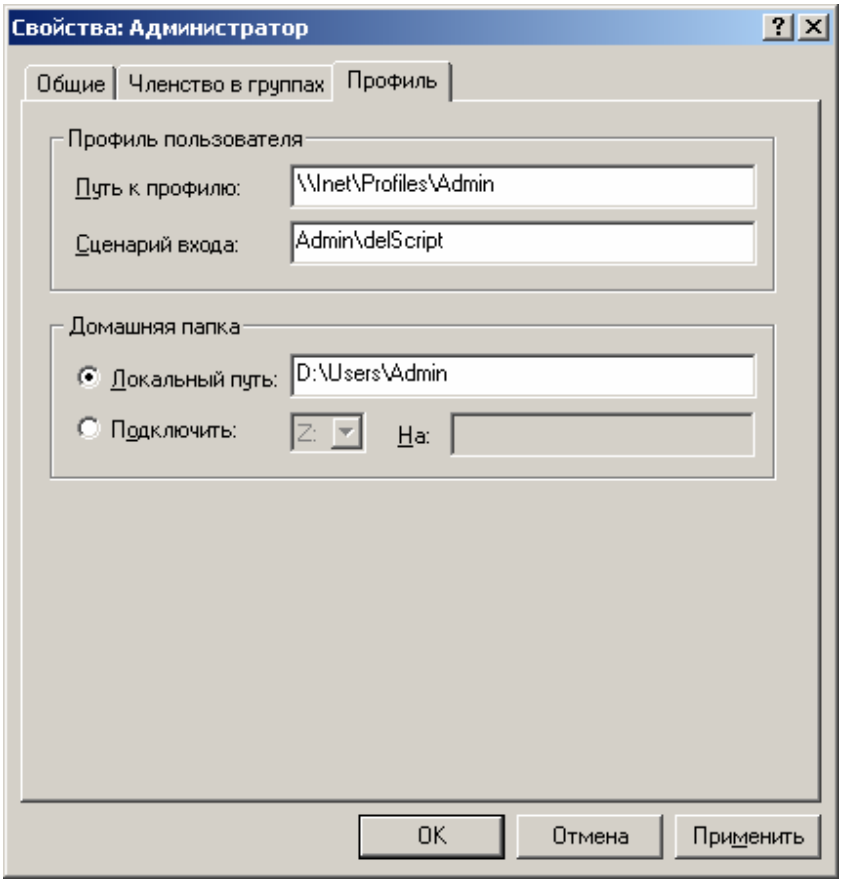

Рис. 16. Вкладка **Профиль** (Profile) окна свойств учетной записи

При первой регистрации вместо профиля, установленного по умолчанию, пользователь получит копию заранее сконфигурированного профиля с сервера. В дальнейшем этот профиль функционирует так же,

как любой стандартный профиль пользователя. Каждый раз, когда пользователь завершает работу, его профиль сохраняется локально и одновременно копируется на сервер.

Примечание. Для копирования профиля пользователя следует перейти на вкладку **Профили** пользователей окна **Система**. Нельзя для этой цели использовать Проводник или какой-либо другой инструмент управления файлами!

Обязательный профиль представляет собой сконфигурированный

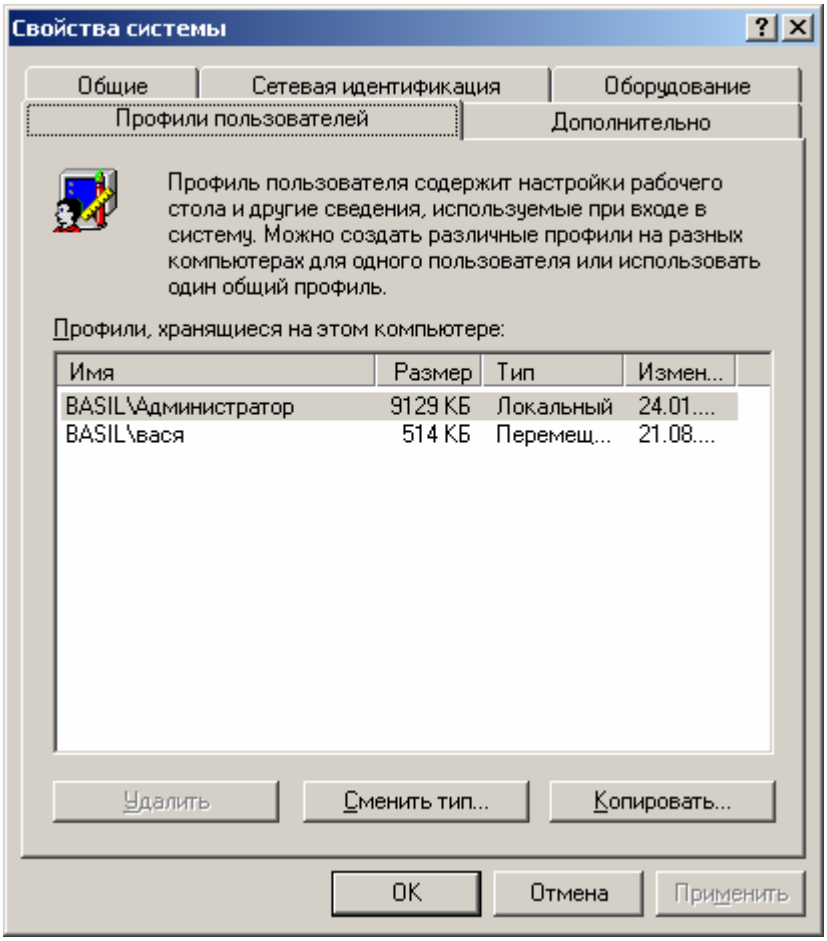

Рис. 17. Окно **Свойства системы** со списком созданных на компьютере профилей пользователя

заранее перемещаемый профиль, который недоступен пользователю для модификации. Пользователь может изменять настройки рабочего стола, но при завершении работы на компьютере изменения не заносятся в профиль. При следующей регистрации на компьютере загружается обязательный профиль пользователя, в котором не произошло никаких изменений. Профиль пользователя становится обязательным, когда вы переименовываете файл NTuser.dat в NTuser.man. В этом случае файл становится доступен только для чтения. Один обязательный профиль может быть использован большим количеством пользователей.

Примечание. Когда для обеспечения безопасности или приведения рабочей среды пользователя в соответствии с его уровнем подготовки для работы на компьютере необходимо контролировать набор доступных функций, лучше использовать групповые политики. С их помощью вы можете выбрать подмножество настроек, а также контролировать как параметры среды *пользователя,* так и настройки компьютера.

Указание пути к профилю пользователя в учетной записи

Добавить путь расположения профиля пользователя к учетной записи можно с помощью вкладки **Профиль** окна свойств пользователя, открытого для определенной учетной записи в окне оснастки **Локальные пользователи и группы** (или **Пользователи и компьютеры Active Directory).** Перейдите вкладку **Профиль** и добавьте путь к профилю пользователя (рис. 16).

В учетной записи следует указать полный путь к профилю пользователя:

*сервер**имя_ общего_ ресурса**имя_ профиля*

В качестве общего ресурса может выступать любая папка, к которой организовать общий доступ для группы Все (Everyone). В качестве имени профиля следует указать имя папки профиля данного пользователя (это может быть любая папка на общем ресурсе, в которой будет храниться профиль).

Путь профиля пользователя может указывать на любой сервер. Это обязательно должен быть контроллер домена. Когда пользователь регистрируется в сети, Windows 2000 Server проверяет, указан ли в его учетной записи путь профиля. Если путь указан, система находит соответствующий профиль.

Копирование профиля пользователя на сервер

Для того чтобы сделать определенный профиль доступным для нескольких пользователей, скопируйте его на сервер с помощью вкладки

Профили окна **Система,** вызываемого из панели управления. Место, куда скопирован профиль, должно совпадать с путем профиля, указанным в учетных записях пользователей.

В окне диалога **Свойства системы** (System Properties) перейдите на вкладку **Профили пользователей.** Все профили пользователей, созданные на компьютере, появятся в списке **Профили, хранящиеся на этом компьютере** (Profiles stored on this computer).

Для копирования определенного профиля пользователя перейдите на вкладку **Копировать** и введите имя целевой папки. В качестве альтернативы можно выбрать целевую папку с помощью службы просмотра. На рис. 17 показан пример окна **Свойства системы** со списком созданных на компьютере профилей пользователя.

Добавление пользователей и групп к списку разрешений перемещаемого профиля пользователя

С помощью окна **Система** вместе с профилем пользователя копируются соответствующие разрешения. Поэтому пользователь автоматически получает доступ к своему профилю. Однако если вы хотите, чтобы к профилю получили доступ другие пользователи и группы, необходимо добавить их в список объектов, которым разрешено использовать данный профиль. Для этого в списке **Профили, хранящиеся на этом компъютере** выберите интересующий вас профиль и нажмите кнопку **Копировать.** Появится окно диалога **Копирование профиля** (Copy To) (рис.18). В группе **Разрешить использование** (Permitted to use) показано, кто имеет разрешение на использование данного профиля. Для того чтобы добавить нового пользователя или группу к списку разрешений профиля пользователя, нажмите кнопку **Изменить** (Change).

Примечание. Если вы назначаете путь перемещаемого профиля пользователя группе, то при каждом завершении работы кого-либо из членов группы его настройки записываются в хранящийся централизованно профиль. По этой причине рекомендуется делать такие профили пользователя обязательными или устанавливать различные настройки разным группам с помощью системных политик.

Подготовка заранее настроенных перемещаемых и обязательных профилей пользователя

Хотя для создания заранее сконфигурированного перемещаемого и обязательного профиля можно использовать любую учетную запись, часто удобнее другой подход. Например, если вы хотите создать 3 различных заранее настроенных перемещаемых или обязательных профиля для 3 отделов предприятия, следует сначала создать и настроить три различные базовые учетные записи. Затем необходимо зарегистрироваться с помощью каждой из созданных учетных записей и тем самым создать три профиля пользователя для трех отделов. после этого опять зарегистрироваться с помощью учетной записи администратора и, используя оснастку **Локальные пользователи и группы,** назначить созданные профили индивидуальным пользователям или группам. Затем с помощью вкладки **Профили пользователей** окна **Система** панели управления скопируйте созданные профили на соответствующий сервер.

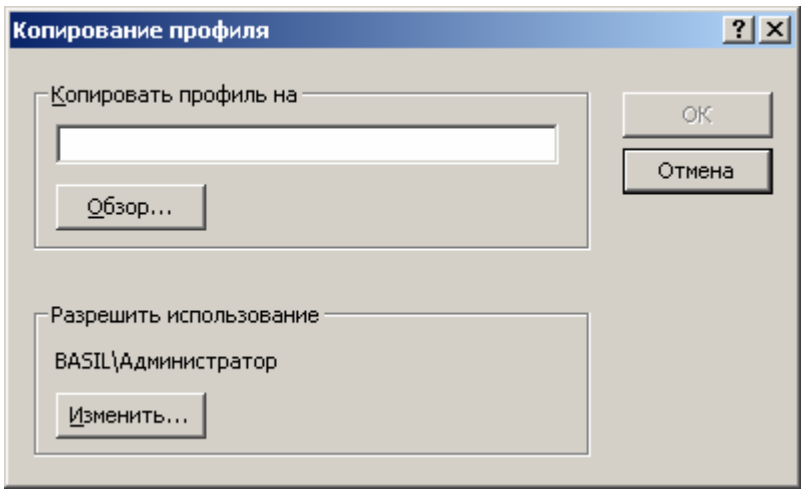

Рис. 18. Окно диалога **Копирование профиля**

Настройка рабочей среды пользователя с помощью сценариев входа

Сценарии входа выполняются автоматически в процессе каждой регистрации пользователя на компьютере, работающем с программным обеспечением Windows 2000. Хотя чаще всего сценарий входа

представляет собой командный файл с рсширением .bat или .cmd, в качестве сценария может быть использован и исполняемый файл (расширение .com или .exe).

Сценарии входа не являются обязательными. Они могут применяться для настройки рабочей среды пользователя, создания сетевых соединений или запуска приложений. Сценарии входа очень удобны, если необходимо изменить некоторые параметры рабочей среды пользователя без выполнения ее полной настройки.

Примечание. Профили пользователя могут в процессе регистрации восстанавливать существовавшие ранее соединения с сетью, но они не могут быть использованы для создания новых соединений.

Создание сценариев входа

Для создания сценариев входа может быть использован обыкновенный текстовый редактор. Затем с помощью оснастки **Локальные пользователи и группы** (Local Users and Groups) сценарии входа назначаются соответствующим пользователям. Кроме того, один сценарий *может* быть назначен нескольким пользователям. В табл. 5 приведены параметры, значения которых можно устанавливать с помощью сценария входа и их описания.

Параметры, устанавливаемые с помощью сценария входа

Таблица 5

Параметр	Описание
%HOMEDRIVE%	Имя устройства локального компьютера, связанного с домашним каталогом пользователя
%HOMEPATH%	Полный путь к домашнему каталогу пользователя
%HOMESHARE%	Имя общего ресурса, где находится домашний каталог пользователя
%OS%	Операционная система компьютера пользователя

Параметр	Описание
%PROCESSOR_ARCHITECTURE%	Тип процессора (например, Pentium) компьютера пользователя
%PROCESSOR_LEVEL%	Уровень процессора компьютера пользователя
%USERDOMAIN%	Домен, в котором находится учетная запись пользователя
%USERNAME%	Имя пользователя

Назначение сценариев входа учетным записям пользователей и групп

Для того чтобы назначить сценарий входа учетным записям пользователей и групп, с помощью оснастки **Локальные пользователи и группы** указывается путь к сценарию. Если при регистрации пользователя с помощью определенной учетной записи среди ее параметров указан путь к сценарию входа, соответствующий файл сценария открывается и выполняется.

На вкладке **Профиль** окна свойств учетной записи вы можете назначить сценарий входа, введя в поле **Сценарий входа** (Logon Script) имя файла (и, возможно, относительный путь к нему). При регистрации сервер, аутентифицирующий пользователя, находит файл сценария (если таковой существует) с помощью указанного в учетной записи имени и пути (на контроллерах домена, как правило, сценарии хранятся в общей папке NETLOGON – %SystemRoot%SYSVOL\sysvol\DNS-имя-домена\scripts). Если перед именем файла указан относительный путь, сервер ищет сценарий входа в подкаталоге основного локального пути сценариев.

Данные поля **Сценарий входа** определяют только имя файла и относительный путь, но не содержат сам сценарий входа. После создания файл сценария с определенным именем помещается в соответствующий каталог.

Сценарий входа можно поместить в локальный каталог компьютера пользователя. Но подобный подход, как правило, применяется только при администрировании учетных записей, существующих на одиночном компьютере, а не в домене. В этом случае

вы должны поместить файл сценария в соответствии с локальным путем к сценариям входа в компьютер.

Помимо осиастки **Локальные пользователи и группы**, сценарии входа могут быть назначены пользователям или компьютерам и с помощью оснастки **Групповая политика** (Groцp Po1icy).

Переменные среды

Изменение системных и пользовательских переменных среды

Для конфигурирования, поиска, выделения памяти определенным программам управления приложениями операционная система Windows 2000 и прикладные программы требуют определенной информации, называемой *леременными среды* системы и пользователя. Их можно просмотреть на вкладке **Дополнительно** (Advanced) окна **Система,** нажав кнопку **Переменные среды** (Environment Variables). Эти переменные похожи на переменные, которые устанавливались в операционной системе MS-DOS, например, PATH и TEMP.

Системные переменные среды определяются в Windows 2000 независимо от того, кто зарегистрировался на компьютере. Если вы зарегистрировались как член группы Администраторы, то можете добавить новые переменные или изменить их значения.

Переменные среды пользователя устанавливаются индивидуально для каждого пользователя одного и того же компьютера. Сюда включаются любые переменные среды, которые вы хотите определить, или переменные, определенные вашим приложением, например, путь к файлам приложения.

После изменения переменных среды их новые величины сохранятся в реестре, после чего они становятся доступны («видны») при закрытии окна **Перемеииые среды.**

Если между переменными среды возникает конфликт, он разрешается следующим способом:

1. Устанавливаются системные переменные среды.
2. Устанавливаются переменные, определенные в файле Auto-exec.bat (за исключением переменных PATH). Они перезаписывают системные переменные.

3. Устанавливаются переменные среды пользователя, определенные в окне **Система.** Они перезаписывают как системные переменные, так и переменные файла Autoexec.bat.

4. Устанавливаются переменные PATH файла Autoexec.bat .

Примечание. Настройки пути (PATH), в отличие от других переменных среды, аддитивны. Полный путь (который вы видите как результат выполнения в командной строке команды path) создается присоединением путей, устанавливаемых в файле Autoexec.bat, к путям, определенным в окне **Система**.

Использование переменных среды в профилях пользователей, именах домашних каталогах и сценариев входа

При управлении множеством учетных записей пользователей и групп часто возникает необходимость одновременно выполнить одинаковые изменения в нескольких учетных записях. Вместо конкретных имен или меток в сценарий входа вводится одна общая переменная среды, замещаемая реальными данными в процессе выполнения сценария.

Значение любой переменной среды компьютера клиента, где работает программное обеспечение Windows 2000, может быть подставлено в путь профиля, задаваемого в учетной записи пользователя, путь сценария входа, путь домашнего каталога и в сам сценарий входа. Для этого системную переменную среды следует заключить в знаки процента (%). Например, для того чтобы использовать в пути профиля пользователя переменную среды Servername, в поле **Путь к профилю** (Profile Path) окна учетной записи следует ввести \\%Servername%\scripts.

Аудит локальной системы

Как уже говорилось в разделе, посвященном безопасности ОС, аудит – это процесс, позволяющий фиксировать события, происходящие в операционной системе и имеющие отношение к безопасности. Например, попытки создать объекты файловой системы, получить к ним доступ или удалить их. Информация о подобных событиях заносится в файл *журнала событий операционной системы.*

После включения аудита операционная система Windows 2000 начинает отслеживать события, связанные с безопасностью. Полученную в результате информацию можно просмотреть с помощью оснастки **Просмотр событий** (Event Viewer). В процессе настройки аудита необходимо указать, какие события должны быть отслежены. Информация о них помещается в журнал событий. Каждая запись журнала

хранит данные о типе выполненного действия, пользователе, выполнившем его, а также о дате и моменте времени выполнения данного действия. Аудит позволяет отслеживать как успешные, так и неудачные попыгки выполнения определенного действия, поэтому при просмотре журнала событий можно выяснить, кто предпринял попытку выполнения неразрешенного ему действия.

Аудит представляет собой многошаговый процесс. Сначала его следует активизировать с помощью оснастки **Групповая политика** (Group Po1icy). (По умолчанию аудит отключен, поскольку он снижает производительность системы.) После включения аудита необходимо определить набор отслеживаемых событий. Это могут быть, например, вход и выход из системы, попытки получить доступ к объектам файловой системы и т. д. Затем следует указать, какие конкретно объекты необходимо подвергнуть аудиту и включить его с помощью Редактора списков управления доступом, ACL

Примечание. Для того чтобы иметь возможность настраивать аудит для файлов и папок, необходимо иметь права администратора.

Аудит, установленный для родительской папки, автоматически наследуется всеми вновь созданными дочерними папками и файлами. Этого можно избежать, если при создании файла или папки вызвать окно свойств и на вкладке **Аудит** (Audit) снять флажок **Переносить наследуемый от родительского объекта аудит на этот объект** (Allow inheritable auditing entries from parent to propagate to this object). Если же этот флажок отображен серым цветом или кнопка **Удалить** недоступна, это значит, что настройки аудита уже унаследованы. В этом случае для изменения настроек аудита дочерних объектов нужно изменить настройки аудита родительской папки, и они будут наследоваться всеми дочерними объектами.

Активизация аудита с помощью оснастки *Групповая политика (GroupPolicy*)

Для активизации аудита на изолированном компьютере:

1. Запустите оснастку **Групповая политика** (это изолированная оснастка, которую можно использовать как самостоятельный инструмент). (Можно выполнить команду **Пуск | Программы | Администрирование | Локальная политика безопасности**.)

2. Откройте папку **Конфигурация компьютера** (Computer Configuration) и последовательно раскройте узлы **Конфигурация Windows** (Windows Configuration), **Параметры безопасности** (Security Settings), **Локальные политики (**Local Policies**)**, **Политика аудита** (Audit Policy). Появившееся окно показано на рис. 19.

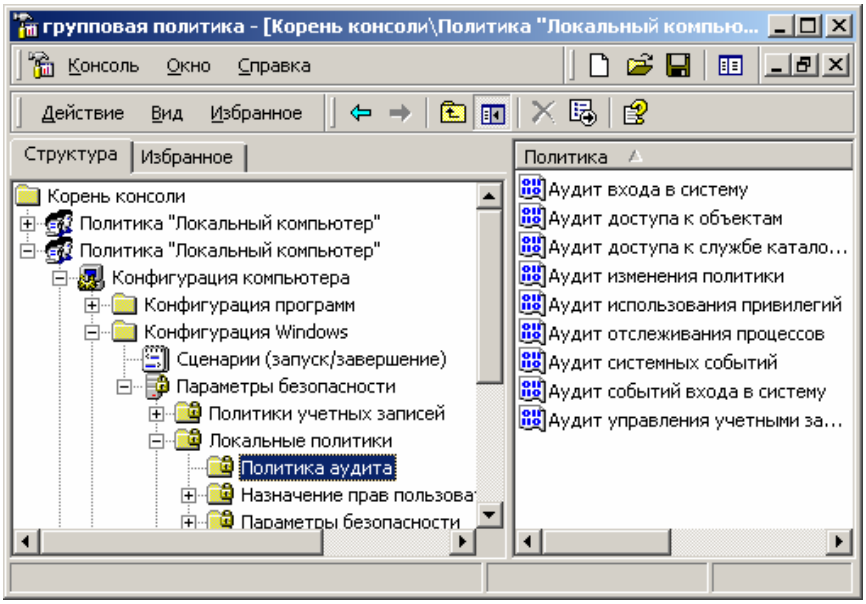

Рис. 19. Окно подключения аудита в системе

3. На правой панели появится список политик аудита. По умолчанию все они имеют значение **Нет аудита** (No Auditing). Для включения аудита следует изменить значения нужных параметров.

4. Выполните двойной щелчок на устанавливаемой политике аудита. Появится окно диалога, с помощью которого можно разрешить аудит. В группе **Вести аудит следующих попыток доступа** (Audit these attempts) установите флажки **Успех** (Success) или **Отказ** (Failure), или оба.

5. Нажмите кнопку **ОК**.

Подобную операцию следует повторить для политик аудита, которые вы хотите активизировать. Для того чтобы отключить аудит, следует снять фдажки **Успех и Отказ.**

Настройка и просмотр аудита файлов и папок

Чтобы настроить, просмотреть или изменить настройки аудита файлов и папок:

1. Установите указатель мыши на файл или папку, для которой следует выполнить аудит, и нажмите правую кнопку. В появившемся контекстном меню выберите команду **Свойства.** В окне свойств папки или файла перейдите на вкладку **Безопасность** (Security).

2. На вкладке **Безопасность** нажмите кнопку **Дополнительно** (Advanced) и затем перейдите на вкладку **Аудит**.

3. Если вы хотите настроить аудит для нового пользователя или группы, на вкладке **Аудит** нажмите кнопку **Добавить.** Появится диалоговое окно **Выбор: Пользователь, Компьютер или Группа** (Select user? computer or group). Выберите имя нужного пользователя или группы и нажмите кнопку **ОК.** Откроется окно диалога **Элемент аудита для** (Audit Entry for). Здесь вы сможете ввести все необходимые параметры аудита. В списке **Применить** (App1y onto) укажите, где следует выполнять аудит (это поле ввода доступно только для папок). В группе **Доступ** (Access) следует указать, какие события следует отслеживать: окончившиеся успешно **(Успех,** Successfull), неудачно **(Отказ,** Failed) или оба типа событий. Флажок **Применять этот аудит к объектам и контейнерам только внутри этого контейнера** (App1y this audit entries to objects and/or containers within this container only) определяет, распространяются ли введенные вами настройки аудита на файлы и папки, находящиеся ниже по дереву каталогов файловой системы (флажок не установлен). В обратном случае установите флажок (или выберите в списке **Применять** опцию **Только для этой папки).** Это позволит не выполнять аудит для тех объектов файловой системы, которые не представляют интереса. После завершения настройки аудита для папки или файла нажмите несколько раз кнопку **ОК,** чтобы закрыть все окна диалога.

4. Если вы хотите просмотреть или изменить настройки аудита для уже существующего пользователя или группы, нажмите кнопку **Показать/Изменить** (View/Edit). Появится окно диалога **Эле-**

мент аудита для. Здесь вы сможете выполнить все необходимые изменения параметров аудита для выбранного вами пользователя или группы. По окончании внесения изменений нажмите кнопку **ОК**.

Отключение аудита файлов и папок

Для отключения аудита файла или папки :

1. Установите указатель мыши на файл или папку, где необходимо отключить аудит, и нажмите правую кнопку. В появившемся меню выберите команду **Свойства**. Появится окно свойств файла или папки. Перейдите на вкладку **Безопасность.**
2. На вкладке **Безопасность** нажмите кнопку **Дополнительно**. В появившемся окне диалога выберите кнопку **Аудит**.
3. В поле **Элементы аудита** выберите нужную запись и нажмите кнопку **Удалить**. Соответствующая запись будет удалена.

Если кнопка **Удалить** недоступна, это значит, что настройки аудита наследуются от родительской папки.

Выполнение заданий по расписанию

В дополнение к команде AT система Windows 2000 располагает новым средством – планировщиком заданий (Task Scheduler). С помощью планировщика заданий можно составить расписание запуска командных файлов, документов, обычных приложений или различных утилит для обслуживания системы. Программы могут запускаться однократно, ежедневно, еженедельно или ежемесячно в заданные дни, при загрузке системы или регистрации в ней, а также при бездействии системы (idle state). Планировщик позволяет задавать достаточно сложное расписание для выполнения заданий, в котором задаются продолжительность задания, время его окончания, количество повторов, зависимость от состояния источника питания (работа от сети или от батарей) и т. п.

Задание сохраняется как файл с расширением .job, что позволяет перемещать его с одного компьютера на другой. Администраторы могут создавать файлы заданий для обслуживания систем и переносить их в нужное место. К папке заданий можно обращаться удаленно, кроме того, задания можно пересылать по электронной почте.

Служба планировщика заданий (Task Scheduler Service, MSTask.exe) инсталлируется вместе с системой и автоматически запускается при ее загрузке. При помощи меню **Дополнительно**

(Advanced) планировщика заданий можно приостанавливать или запускать снова эту службу. Данное меню позволяет также обращаться к журналу регистрации запланированных и выполненных заданий.

Среди особенностей планировщика можно отметить:

- удобный графический пользовательский интерфейс;
- возможность программного доступа ко всем возможностям планировщика, включая страницы свойств;
- создание новых заданий при помощи технологии drag-and-drop или мастера планирования заданий *(Scheduled Task wizard);*
- средства безопасности.

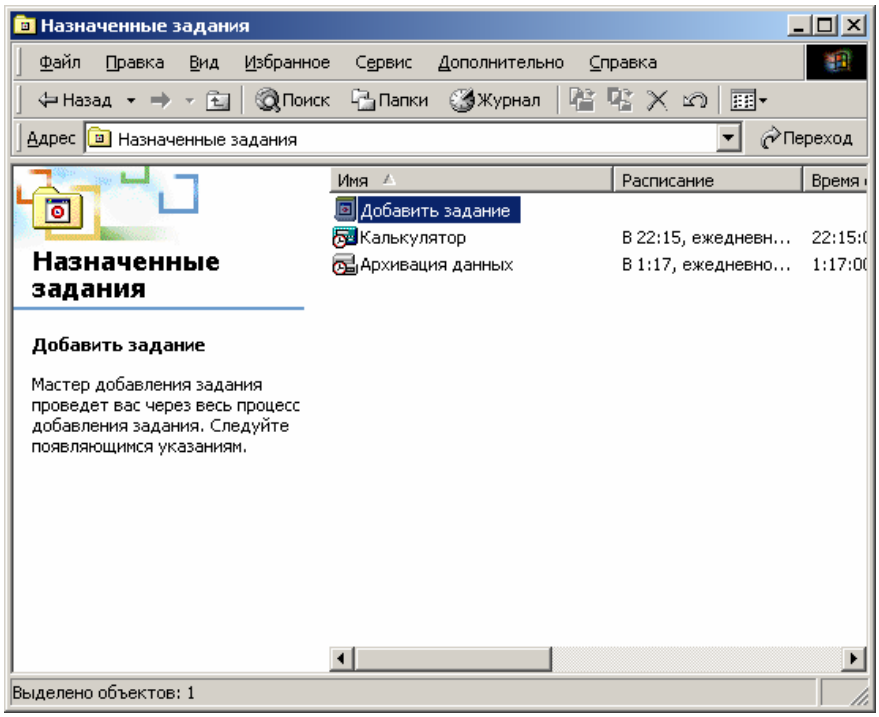

Рис. 20. Главное окно программы Планировщик заданий со списком запланированных заданий

Графический интерфейс планировщика заданий (рис. 20) не требует знания ключей и параметров программы (как это нужно для

использования команды AT), интегрирован в операционную систему и доступен из панели управления (папка **Назначенные задания** (Scheduled Tasks)). Кроме того, упрощается отладка заданий, поскольку их легко проверить, запустив в любой момент непосредственно из папки заданий (команда **Выполнить** (Run) в контекстном меню). В главном окне планировщика выводится основная информация о заданиях: расписание, время следующего и предыдущего запуска, состояние, результат выполнения задания, имя создателя задания.

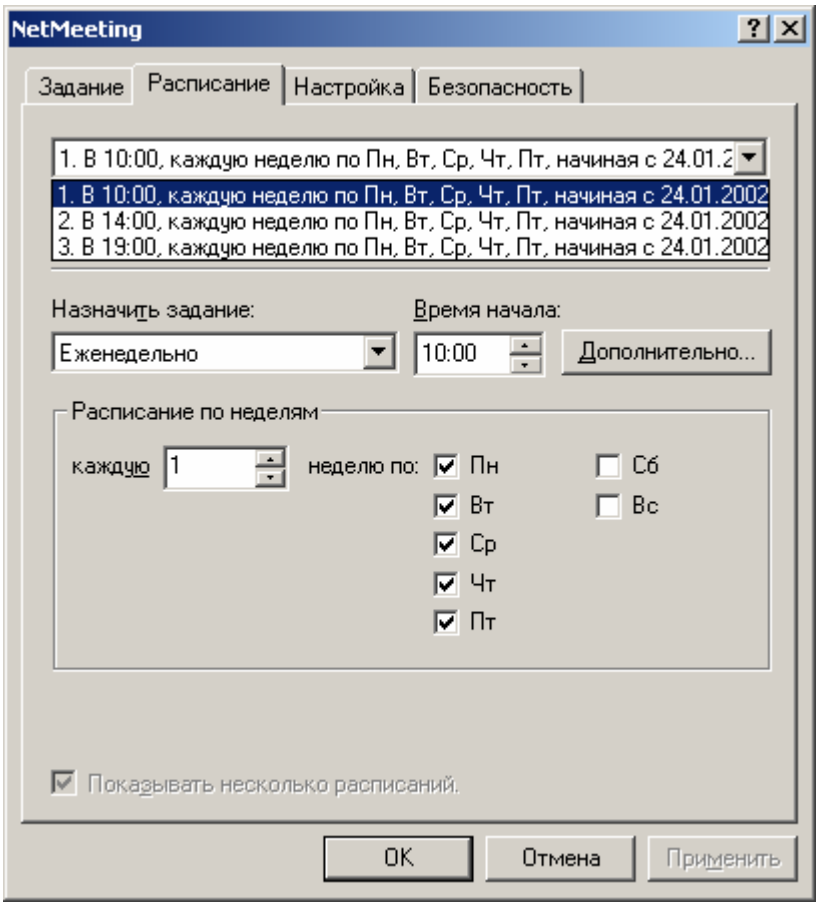

Рис.21. Вкладка **Расписание** для запланированного запуска программы NetMeeting

Мастер планирования заданий (запускаемый при выборе команды **Добавить задание** (Add Scheduled Task)) позволяет легко и быстро в интерактивном режиме указать все параметры для запуска запланированного задания. Задания могут иметь несколько расписаний, принципиально отличающихся друг от друга. Например, некоторая программа может запускаться ежедневно в одно время, еженедельно – в другое время и однократно – в заданное время указанного дня. На рис. 19 приведен пример расписания для запуска программы NetMeeting, запускающейся по рабочим дням, 3 раза в день. Установив флажок **Показывать несколько расписаний** (Show multiple schedules), можно задавать несколько расписаний для запуска этой программы.

В среде Windows 2000 запланированные задания создаются и выполняются с учетом стандартных разрешений системы безопасности. На файлы заданий распространяются правила использования списков управления доступом (ACL) файловой системы NTFS, определяющие круг лиц, которым разрешено просматривать, удалять, модифицировать и выполнять задания (обратите внимание на вкладку **Безопасность** (Security), рис. 21).

11. РАБОТА С ОБЩИМИ ДИСКОВЫМИ РЕСУРСАМИ

Локальное и удаленное администрирование общих ресурсов в Windows 2000 осуществляется с помощью оснастки **Общие папки** (Shared Folders). В Windows NT аналогичные функции выполняла утилита Server панели управления. С ее помощью можно также управлять сеансами и открытыми файлами. Она входит в стандартный инструмент администрирования - **Управление компьютером** (Computer Management). Ниже мы рассмотрим, как с помощью оснастки **Общие папки** можно создать общий ресурс.

*Оснастка **Общие папки***

Для запуска изолированной оснастки **Общие папки** как самостоятельного инструмента:

1. Нажмите кнопку **Пуск** (Start), выберите команду **Выполнить** (Run), введите с клавиатуры **mmc** и нажмите **ОК**.
2. В появившемся окне в меню **Консоль** (Console) выберите команду **Добавить/удалить оснастку** (Add/remove Snap-in).
3. В следующем окне нажмите кнопку **Добавить** (Add).

4. В окне **Добавить изолированную оснастку** (Add Standalone Snap-in) выделите оснастку **Общие папки** и нажмите кнопку **Добавить**.

5. В окне **Общие папки** в группе **Эта оснастка всегда управляет** (This snap-in will always manage) выберите положение переключателя **локальным компьютером** (Local Computer) или **другим компьютером** (Another Computer), если вы хотите работать с другим компьютером в сети. В последнем случае в поле ввода следует указать имя компьютера (или можно воспользоваться кнопкой **Обзор** (Browse)). В группе параметров **Просмотр** (View) укажите, какую информацию (общие ресурсы, сеансы, открытые файлы или все перечисленное) можно будет просматривать с помощью оснастки.

6. Нажмите кнопку **Готово** (Finish).

7. В окне **Добавить изолированную оснастку** нажмите кнопку

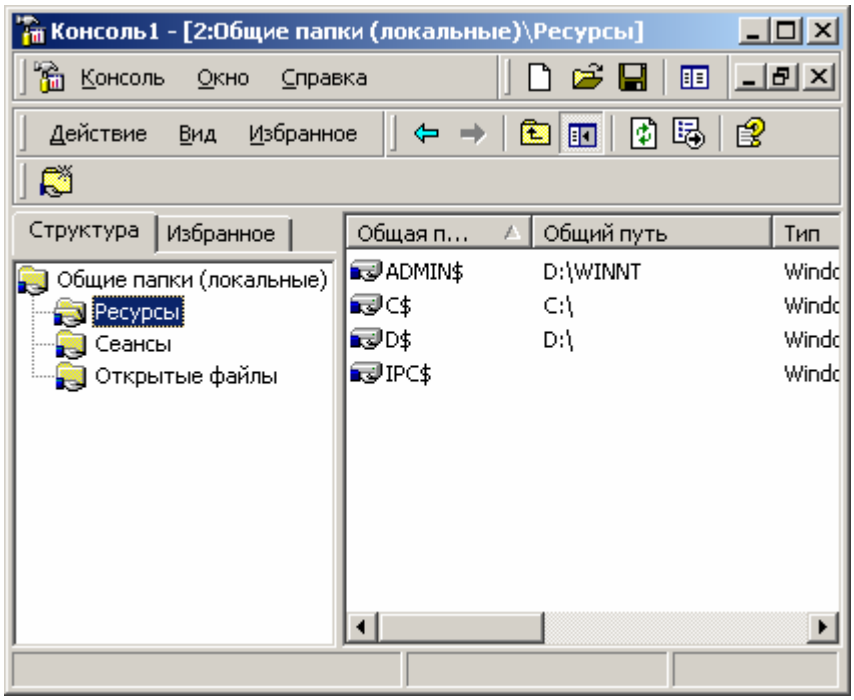

Рис. 22. Окно оснастки **Общие папки** (Shared Folders)

Закрыть (Close)

8. В окне **Добавить/удалить оснастку** нажмите кнопку **ОК -** окно будет закрыто.

Пример окна оснастки **Общие папки** для **локального** компьютера показан на рис. 22.

Для создания общего ресурса:

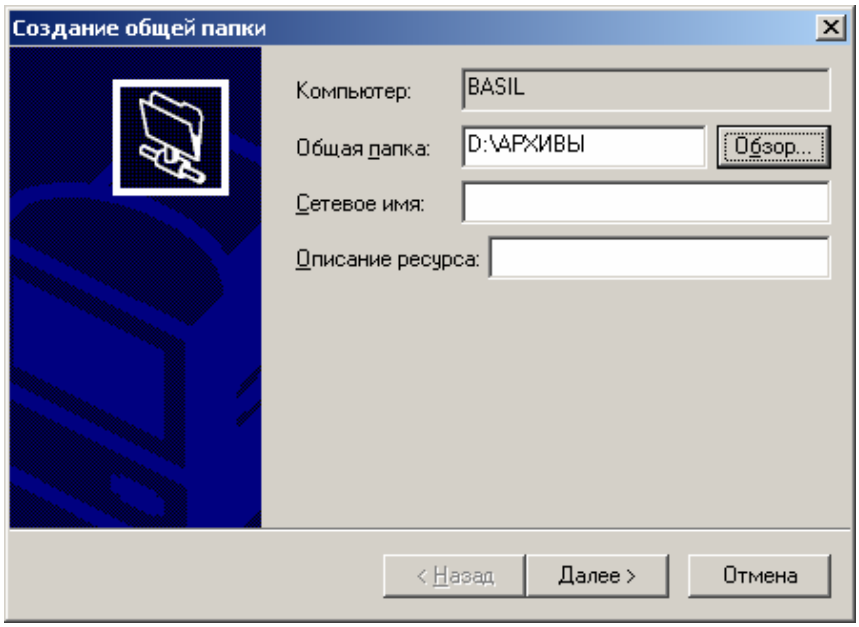

Рис. 23. Окно диалога программы создания общих ресурсов

1. В окне структуры оснастки **Общие папки** установите указатель мыши на папку **Ресурсы** (Shares) и нажмите правую кнопку.

2. В появившемся контекстном меню выберите команду **Новый общий файл** (New File Share).

3. В полях ввода окна **Создание общей папки** (Create Shared Folder), показанном на рис. 23, следует указать имя каталога (это может быть уже существующий каталог или вновь создаваемый), который должен стать общим ресурсом, сетевое имя общего ресурса и описание общего ресурса. Имена каталога и общего ре-

сурса являются обязательными для ввода. Существующий каталог можно выбрать с помощью кнопки **Обзор.** Нажмите кнопку **Далее** (Next).

4. Появится окно (рис. 24), в котором можно выбрать разрешения доступа к создаваемому общему ресурсу (по умолчанию – доступ для всех пользователей разрешен). Выполните все необходимые настройки и нажмите кнопку **Готово.** В появившемся окне нажмите кнопку **Да**, если необходимо создать еще один общий ресурс, или **Нет** – для возврата в основное меню оснастки **Общие папки**.

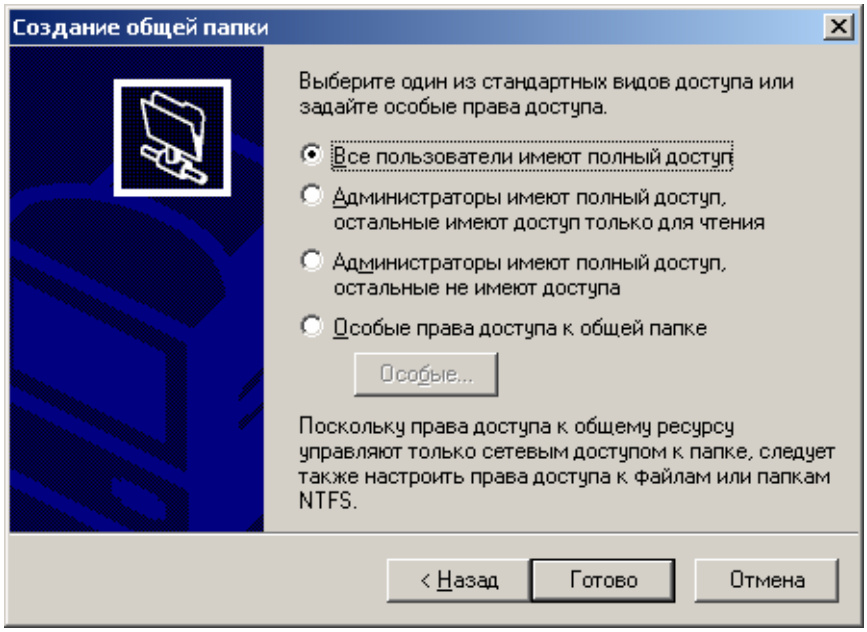

Рис. 24 Настройка разрешений доступа к создаваемому общему ресурсу

Примечание. Рекомендуется на уровне прав доступа к общему ресурсу задавать наиболее *«широкие»* права (если позволяют требования безопасности – полный доступ для всех), а затем настраивать более *«узкие»* права доступа к файлам и папкам на уровне файловой системы NTFS. Такой подход упрощает администрирование прав пользователей.

Хотя Windows 2000 и поддерживает файловую систему FAT, для более высокой безопасности, надежности и легкости в

администрировании, рекомендуется использовать файловую систему NTFS. Посмотреть, какая файловая система используется в настоящий момент, можно в окне свойств диска или с помощью оснастки **Управление дисками** (Disk Management).

Свойства уже созданного общего ресурса могут быть модифицированы следующим образом:

1. Установить указатель мыши на общий ресурс, свойства которого вы хотите модифицировать, и нажмите кнопку.

2. В появившемся контекстном меню выберите команду **Свойства** (Properties). Появится окно свойств общего ресурса (рис. 25), в котором можно менять его существующие параметры.

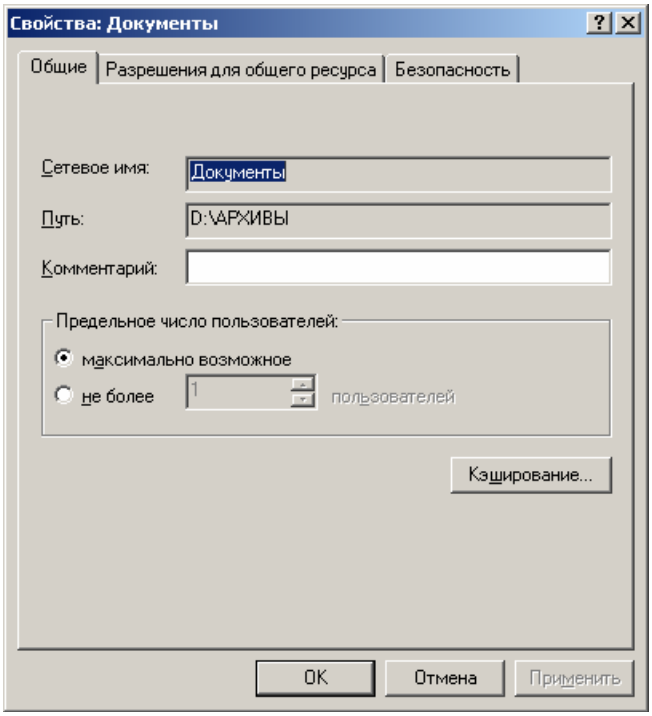

Рис. 25. Окно свойств общего ресурса

Другие способы создания общих дисковых ресурсов

В Windows NT 4.0 создание и администрирование общих ресурсов (в том числе и дисковых) обычно осуществлялось с помощью программы

Проводник (Windows Explorer) и окна свойств ресурса. Создание общих ресурсов и управление ими (настройка разрешений) с помощью Проводника поддерживается и в Windows 2000, так же, как и применение для этой цели команды net share. Могут быть применены и другие инструменты, использующие Win32 API. Однако для централизованного и удаленного администрирования общих ресурсов оснастка **Общие папки** более удобна.

Автономные файлы

Что делать, если пользователю необходимо работать с документами, находящимися в общем каталоге, в условиях отсутствия соединения с сетью? Операционная система Windows 2000 располагает средством *Автономные фай*лы (Offline Files), позволяющим решать подобные проблемы. С его помощью пользователи могут открывать и корректировать файлы, находящиеся в общих папках, даже отключившись от сети.

При отключении от сети автономные файлы извещают об этом пользователя. В панели задач появляется специальный значок, а на рабочем столе – сообщение, сигнализирующее о том, что сетевое соединение исчезло и началась автономная работа. При конфигурировании автономных файлов пользователь может сам выбрать, как они должны реагировать на отключение от сети. После подключения к сети Диспетчер синхронизации (Synchronization Manager) переносит все изменения, сделанные пользователем в сетевых файлах в процессе автономной работы, на общий сетевой ресурс.

При автономной работе, не имея соединения с сетью, пользователь не теряет способности просматривать сетевые устройства и работать со своими файлами. На значках отключенных сетевых общих ресурсов появляется красный крестик. Просматривая эти ресурсы, пользователи смогут увидеть только те файлы, которые были заранее указаны или которые были открыты ими недавно, до разрыва соединения.

Права доступа в автономном режиме работы остаются такими же, какие они были при наличии соединения с сетью. Например, документ, доступный на сетевом общем ресурсе только для чтения, будет доступен только для чтения и при автономной работе.

Для того чтобы сделать доступными для пользователей, отключенных от сети, файлы общих ресурсов, нужно поместить их в кэш компьютера. Кэш компьютера – это часть пространства диска, доступ к которому возможен в любом состоянии соединения с сетью. Автономные файлы позволяют применять три варианта кэширования (это задается на

вкладке **Доступ** (Sharing) в окне свойств общего ресурса – кнопка **Кэширование** (Cashing)):

- *ручное* кэширование для документов (Manual Cashing for Documents);
- *автоматическое* кэширование для документов (Automatic Cashing for Documents);
- автоматическое кэширование для *программ* (Automatic Cashing for Documents).

Ручное кэширование для документов

Ручное кэширование предполагает, что, отключившись от сети, пользователь сможет открывать только те файлы общего сетевого ресурса, которые он *предварительно указал.* Такой тип кэширования идеален для работы с обшим ресурсом, на котором находятся документы или рисунки. Этот вариант кэширования устанавливается по умолчанию.

Автоматическое кэширование для документов

Автоматическое кэширование позволяет данному пользователю работать автономно с теми файлами, которые он *открывал* на общем сетевом ресурсе. Нет гарантии, что для автономной работы будут доступны *все* файлы, находящиеся в общей папке.

Автоматическое кэширование для программ

Автоматическое кэширование для программ позволяет автономно работать только с теми программами, которые пользователь *запускал,* работая в сети, из общей папки. Рекомендуется для работы с ресурсами, доступными только для чтения.

Настройка компьютера для работы с автономными папками

Для создания автономных папок на компьютере:

1. В окне Проводника или в окне **Мой компьютер** в меню **Сервис** (Too1s) выберите команду **Свойства папки** (Folder Options).
2. В появившемся окне перейдите на вкладку **Автономные файлы** (Offline Files) (рис. 26) и установите флажок **Использовать автономные файлы** (Enable Offline Files).
3. Установив или сняв флажок **Синхронизировать перед выходом из системы** (Synchronize all offline files before logging off), можно

указать на необходимость осуществления синхронизации при выходе.

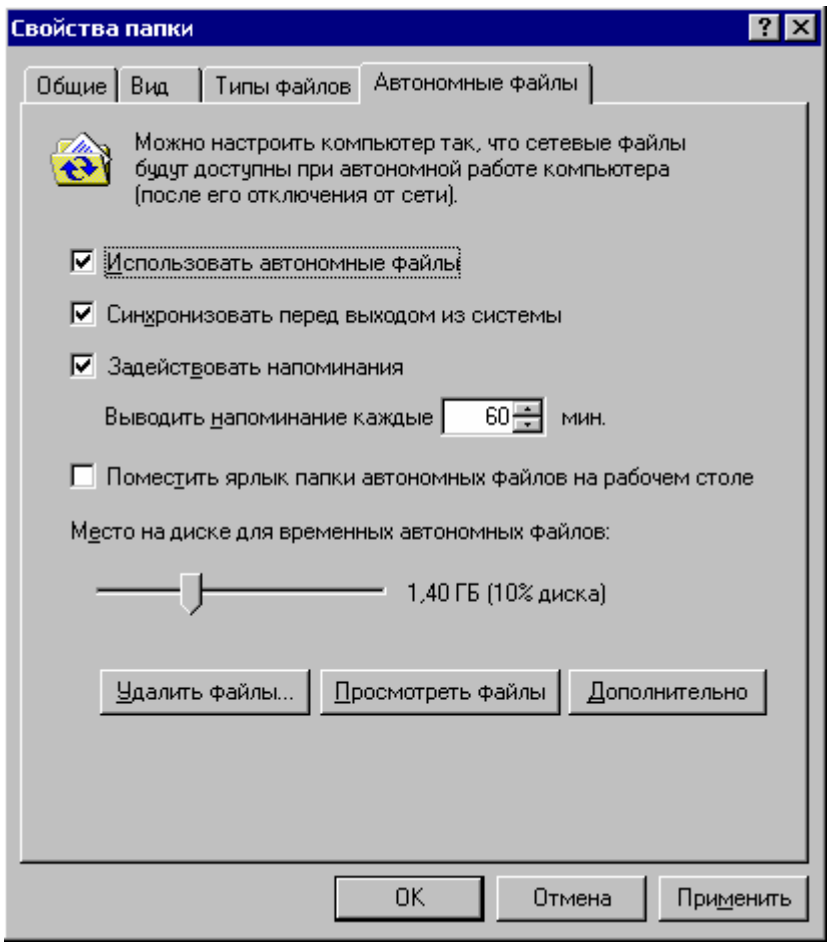

Рис. 26. Вкладка **Автономные файлы** окна **Свойства папки**

По умолчанию на рабочей станции флажок **Использовать автономные файлы** установлен, а на сервере снят. После настройки компьютера для работы с автономными папками следует указать конкретные файлы и папки, с которыми необходимо работать автономно (эта операция описана в следующем разделе). Для выполнения быстрой синхронизации нужно сформировать расписание диспетчера

синхронизации, который осуществляет синхронизацию файлов и папок перед завершением работы компьютера.

Для просмотра списка сетевых файлов и папок, с которыми можно работать автономно, следует нажать кнопку **Просмотреть файлы** (View Files) на вкладке **Автономные файлы.**

Выбор файлов для автономной работы

Для того чтобы обозначить, с какими файлами и папками необходимо работать автономно:

1. Щелкните на значке **Мой компьютер** или **Мое сетевое окружение** (My Network Places). В появившемся окне выделите файлы, находящиеся на сетевых устройствах, с которыми будет выполняться автономная работа.

2. В контекстном меню выберите команду **Сделать доступным в автономном режиме** (Make Available Offline) – запустится Мастер автономных файлов. Следуйте указаниям этой программы. После ввода всей необходимой для создания автономных файлов информации начнется процесс синхронизации. Появится окно синхронизации (рис. 27). Когда оно закроется, указанные файлы и папки будут доступны для автономной работы.

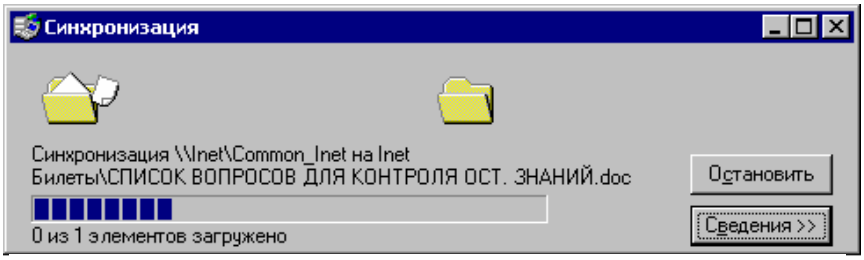

Рис. 27. Окно синхронизации, появляющееся при создании автономной папки

Доступные для автономной работы файлы и папки можно изменять после отключения от сети. Команда **Сделать доступным в автономном режиме** доступна в меню **Файл** только после того, как на вкладке **Автономные файлы** установлен флажок **Использовать автономные файлы.**

Настройка реакции автономных файлов на отключение компьютера от сети

Чтобы определить, как автономные папки будут реагировать на отключение от сети:

1. В окне Проводника или в окне **Мой компьютер** в меню **Сервис** выберите команду **Параметры папки**.

2. В появившемся окне диалога на вкладке **Автономные файлы** нажмите кнопку **Дополнительно**.

3. Появится окно **Автономные файлы – дополнительная настройка** (Offline Files – Advanced Settings) (рис. 28). С его помощью можно настроить реакцию компьютера на потерю сетевого

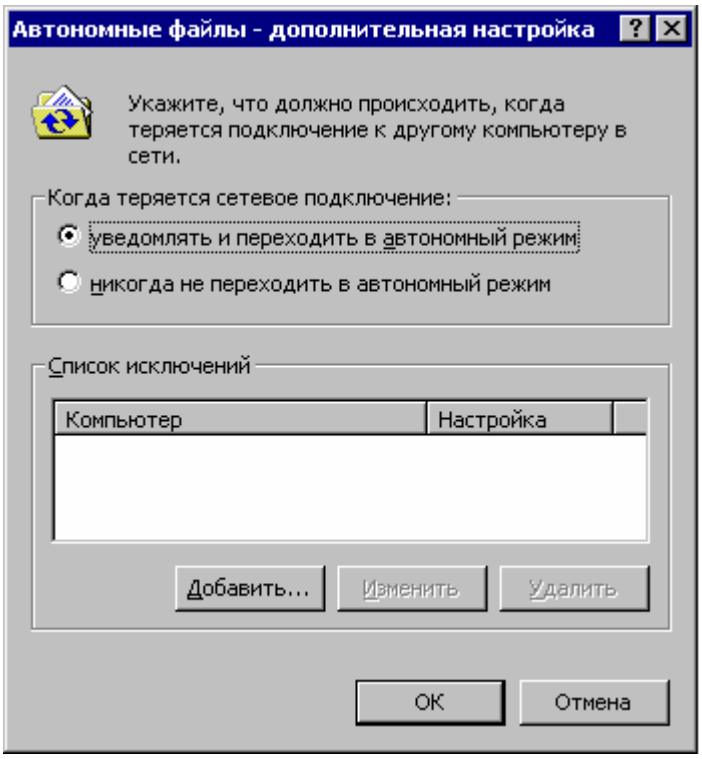

Рис. 28. Окно диалога, предназначенное для настройки реакции автономных файлов на отключение от сети

соединения, для чего в группе **Когда теряется сетевое подклю-**

чение (When a network connection is lost) следует установить соответствующий переключатель.

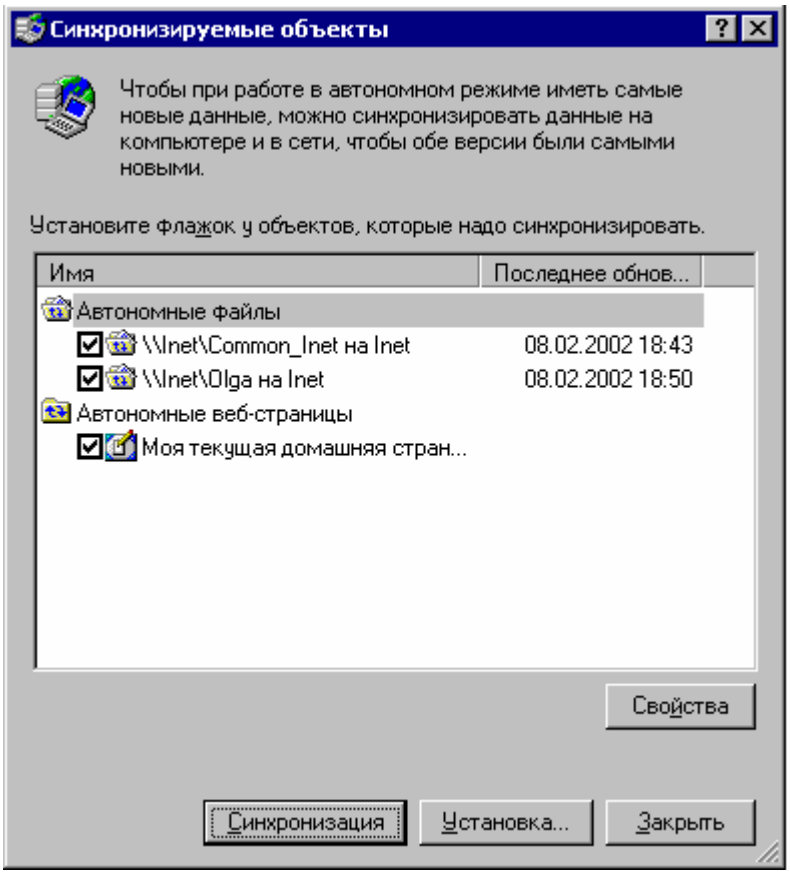

Рис. 29. Выбор синхронизируемых папок и файлов

4. В поле **Список исключений** (Exception List) можно определить список компьютеров, при потере соединения с которыми должны выполняться индивидуальные настройки реакции автономных файлов. Добавить компьютер в список исключений можно, нажав кнопку **Добавить.** В появившемся диалоговом окне следует указать имя компьютера, обладающего индивидуальными настройками реакции автономных папок, и действие при отключении от сети.

Синхронизация информации автономных папок и общего ресурса

Поскольку отключение компьютера от сети дает возможность пользователю продолжать корректировать свои файлы в автономных папках, а все пользователи, компьютеры которых не потеряли соединения с сетью, продолжают работать с файлами общего ресурса сети, содержимое одних и тех же файлов становится различным. Поэтому после восстановления соединения с сетью необходимо выполнить синхронизацию автономных папок и общего сетевого ресурса.

Синхронизация информации может быть выполнена тремя способами:

- принудительная синхронизация;
- синхронизация в процессе регистрации на компьютере или завершения работы компьютера;
- синхронизация в момент бездействия компьютера.

Для принудительной синхронизации:

1. Запустите диспетчер синхронизации. Для этого в меню **Сервис** следует выбрать команду **Синхронизировать** (Synchronize).
2. Установите флажки, соответствующие автономным файлам, которые следует синхронизировать (рис. 29).
3. Нажмите кнопку **Синхронизация**. В процессе синхронизации возможны конфликты версий одноименных файлов, располагающихся на локальном компьютере и на общем ресурсе. При этом система выдает сообщения, содержащие информацию о времени корректировки каждого из файлов и запрос на последующие действия. В этих случаях пользователь может выбрать одну из трех возможностей:
    - оставить только ту копию файла, которая хранится на локальном компьютере;
    - оставить только ту копию, которая находится на общем ресурсе;
    - сохранить более позднюю версию файла под новым именем (по умолчанию к имени файла добавляется имя компьютера, откуда берется эта версия).

Для установки синхронизации автономных папок при входе в систему или выходе из системы:

1. Запустите диспетчер синхронизации и нажмите кнопку **Установка** (Setup). Появится окно диалога **Параметры синхронизации** (Synchronization Settings) (рис. 30).

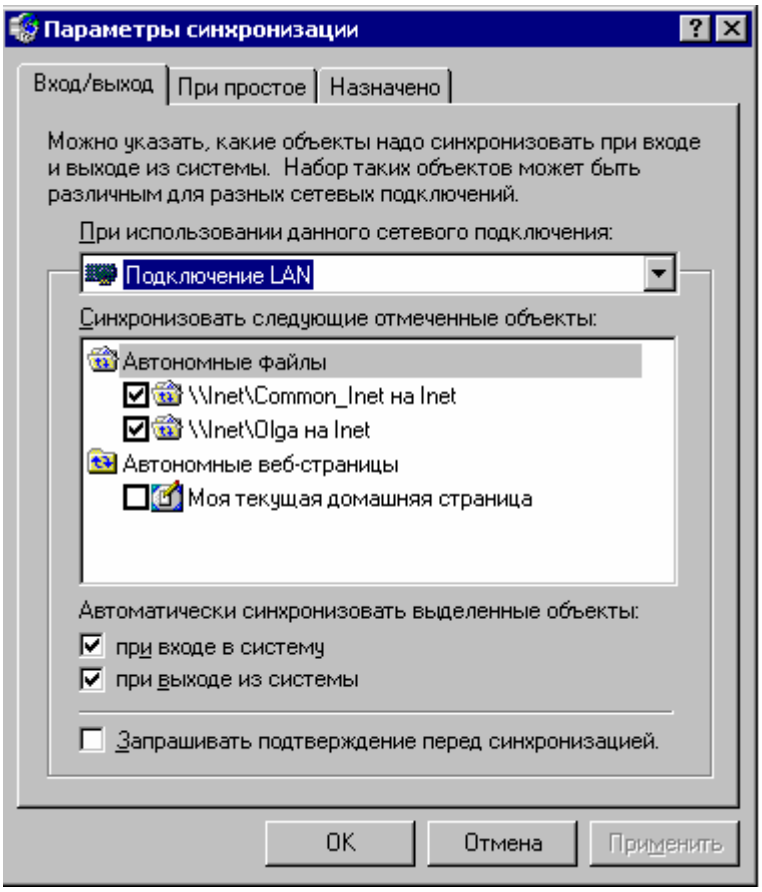

Рис. 30. Настройка параметров синхронизации

2. Перейдите на вкладку **Вход/выход** (Logon/Logout). В поле **При использовании данного сетевого подключения** (When I am using this network connection) выберите сетевое соединение, которое вы хотите использовать.

3. В поле **Синхронизовать следующие отмеченные объекты** (Synchronize the following checked items) установите флажки, соответствующие синхронизируемым объектам.

4. В поле **Автоматически синхронизовать выделенные объекты** (Automatically synchronize the selected items) выберите положение переключателя **при входе в систему** (When I log on to my computer) или **при выходе из системы** (When I log on to my computer) - если вы хотите синхронизировать информацию по завершению работы с системой.

5. Если вы хотите, чтобы диспетчер синхронизации запрашивал у вас разрешения на автоматическую синхронизацию, установите флажок **Запрашивать подтверждение перед синхронизацией** (Ask me before synchronizing the items).

6. После установки параметров закройте окно диспетчера синхронизации.

Для синхронизации информации автономных папок в момент бездействия компьютера нужно в окне **Параметры синхронизации** перейти на вкладку **При простое** (On Idle), выбрать нужное сетевое подключение и установить флажки около синхронизируемых файлов. По умолчанию синхронизация отмеченных файлов начинается, если компьютер не используется 15 минут, и повторяется каждый час.

12. СРЕДСТВА БЕЗОПАСНОСТИ WINDOWS 2000

Шифрующая файловая система

На персональном компьютере операционную систему можно загрузить не с жесткого, а с гибкого диска. Это позволяет обойти проблемы, связанные с отказом жесткого диска и разрушением загрузочных разделов. Однако, поскольку с помощью гибкого диска можно загружать различные операционные системы, любой пользователь, получивший физический доступ к компьютеру, может обойти встроенную систему управления доступом файловой системы Windows 2000 (NTFS) и с помощью определенных инструментов прочесть информацию жесткого диска. Многие конфигурации оборудования позволяют применять пароли, регулирующие доступ при загрузке. Однако такие средства не имеют широкого распространения. Кроме того, если на компьютере работает несколько пользователей, подобный подход не дает хороших результатов, да и сама защита с помощью пароля недостаточно надежна. Вот типичные примеры несанкционированного доступа к данным:

- *Хищение переносного компьютера.* Любой злоумышленник может похитить переносной компьютер, а затем получить доступ к конфиденциальной информации, находящейся на его жестком диске.

- *Неограниченный доступ.* Компьютер оставлен в рабочем состоянии, и за ним никто не наблюдает. Любой пользователь может подойти к такому компьютеру и получить доступ к конфиденциальной информации.

- Основной целью создания системы безопасности является защита конфиденциальной информации, которая обычно находится в незащищенных файлах на жестком диске, от несанкционированного доступа. Доступ к данным можно ограничить с помощью средств NTFS. Такой подход обеспечивает хорошую степень защиты, если единственной загружаемой операционной системой является Windows 2000, жесткий диск не может быть физически удален из компьютера, и данные находятся в разделе NTFS. Если кто-либо захочет получить доступ к данным, он может осуществить свое желание, получив физический доступ к компьютеру или жесткому диску. Существуют *инструменты, позволяющие получить доступ к файлам, находящимся в разделе NTFS,* из операционных систем MS-DOS или UNIX в обход системы безопасности NTFS.

Из приведенных выше соображений следует вывод: единственный надежный способ защиты информации – это шифрующая файловая система. На рынке программного обеспечения существует целый набор продуктов, обеспечивающих шифрование данных с помощью образованного от пароля ключа на уровне приложений. Однако такой подход имеет ряд ограничений:

- *Ручное шифрование и дешифрование. Службы* шифрования большинства продуктов непрозрачны для пользователей. Пользователю приходится расшифровывать файл перед каждым его использованием, а затем опять зашифровывать. Если пользователь забывает зашифровать файл после окончания работы с ним, информация остается незащищенной. Поскольку каждый раз необходимо указывать, какой файл должен быть зашифрован (и расшифрован), применение такого метода защиты информации сильно затруднено.

- *Утечка информации из временных файлов и файлов подкачки.* Практически все приложения в процессе редактирования документов создают временные файлы. Они остаются на диске незашифрованными, несмотря на то, что оригинальный файл зашифрован. Кроме того, шифрование информации на уровне приложений выполняется в режиме пользователя Windows 2000. Это значит, что ключ, применяе-

мый для такого типа шифрования, может храниться в файле подкачки. В результате, с помощью изучения данных файла подкачки можно получить ключ и расшифровать все документы пользователя.

- *Слабая криптостойкость ключей.* Ключи образуются от паролей или случайных фраз. Поэтому в случае, если пароль был легко запоминаемым, атаки с помощью словарей могут легко привести к взлому системы защиты.

- *Невозможность восстановления данных.* Большинство продуктов, позволяющих шифровать информацию, не предоставляют средств восстановления данных, что для пользователей является дополнительным поводом не применять средства шифрования. Это особенно касается тех работников, которые не хотят запоминать дополнительный пароль. С другой стороны, средство восстановления данных с помощью пароля – еще одна брешь в системе защиты информации. Все, что необходимо злоумышленнику, – это пароль, предназначенный для запуска механизма восстановления данных, который позволит получить доступ к зашифрованным файлам.

Все перечисленные выше проблемы позволяет решить *шифрующая файловая система (Encrypting File System, EFS)*, реализованная в Windows 2000 и работающая только на NTFS 5.0. В следующих разделах подробно описаны место шифрования в операционной системе, взаимодействие с пользователями и способ восстановления данных.

Место EFS в Windows 2000

EFS тесно взаимодействует с NTFS 5.0. Временные файлы, создаваемые приложениями, наследуют атрибуты оригинальных файлов (если файлы находятся в разделе NTFS). Вместе с файлом шифруются также и его временные копии. EFS находится в ядре Windows 2000 и использует для хранения ключей специальный пул, не выгружаемый на жесткий диск. Поэтому ключи никогда не попадают в файл подкачки.

Конфигурация EFS, устанавливаемая по умолчанию, позволяет пользователю шифровать свои файлы без всякого вмешательства со стороны администратора. В этом случае EFS автоматически генерирует для пользователя пару ключей (открытый и личный), применяемую для криптозащиты данных. Шифрование и дешифрование файлов может быть выполнено как для определенных файлов, так и для целого каталога. Криптозащита каталога прозрачна для пользователя. При шифровании каталога автоматически шифруются и все входящие в него файлы и подкаталоги. Каждый файл обладает уникальным ключом, позволяющим

легко выполнять операцию переименования. Если вы переименовываете файл, находящийся в зашифрованном каталоге, и переносите его в незашифрованный каталог, сам файл остается зашифрованным (при условии, что целевой каталог находится на томе NTFS 5.0). Средства шифрования и дешифрования доступны через Проводник. Кроме того, можно использовать все возможности криптозащиты данных с помощью набора утилит командной строки и интерфейсов администрирования.

EFS исключает необходимость предварительного расшифровывания данных при доступе к ним. Операции шифрования и дешифрования выполняются автоматически при записи или считывании информации. EFS автоматически распознает зашифрованный файл и найдет соответствующий ключ пользователя в системном хранилище ключей. Поскольку механизм хранения ключей основан на использовании CryptoAPI, пользователи получают возможность хранить ключи на защищенных устройствах, например, смарт-картах.

Если зашифрованные файлы хранятся на общих ресурсах, то для работы с ними пользователи должны иметь сертификат и личный ключ того, кто установил шифрование этих файлов. Впоследствии каждый пользователь может при необходимости независимо расшифровать файл при помощи своего личного ключа.

Примечание. Будьте внимательны: нельзя шифровать сжатые файлы и папки (и наоборот - сжимать зашифрованные данные)!

Напомним, что каталоги и файлы можно шифровать только на томах NTFS.

Управление сертификатами пользователей

Пользователи могут запрашивать, экспортировать, импортировать сертификаты, служащие в EFS для идентификации пользователей, а также управлять ими. Эта возможность предназначена для опытных пользователей, которые хотят иметь средство управления собственными сертификатами. Обычно пользователям не приходится самостоятельно управлять сертификатами, поскольку EFS автоматически генерирует для них пару ключей при первом обращении к ней, т. е. при попытке зашифровать файл или каталог (при этом открытый ключ сертифицируется в центре сертификации, а если таковой не доступен, то EFS сама подписывает открытый ключ).

В вышесказанном легко убедиться, если после инсталляции системы запустить оснастку **Сертификаты** и раскрыть узел (папку) **Личные:** этот узел будет пуст. Если затем зашифровать некоторый файл

или папку и вернуться в оснастку **Сертификаты,** то можно увидеть, что в папке **Личные** появился сертификат, выданный текущему пользователю.

Управление сертификатами, их импорт и экспорт осуществляется с помощью контекстных меню оснастки **Сертификаты** (Certificates). Пользователи имеют возможность управлять только своими собственными сертификатами.

Если вы зашифровали какую-нибудь информацию, то *обязательно* выполните экспорт сертификата с записью его на дискету! Если вдруг понадобится выполнить заново инсталляцию системы и вы забудете расшифровать эту информацию (что весьма вероятно!), то *доступ к ней навсегда будет утерян.*

'Утилита cipher

Эта утилита командной строки позволяет шифровать и дешифровать файлы. Ниже приведен ее синтаксис, описание ключей дано в табл. 6.

cipher [/E | D] [/S : каталог] [/A] [/I] [/F] [/Q] [/H] [/K/ [путь […]]

Ключи утилиты cipher

Таблица 6

Ключ	Описание
/E	Шифрует указанные в качестве параметра *путь* файлы. Каталоги помечаются как зашифрованные, все файлы, которые будут помещены в них впоследствии, шифруются автоматически
/D	Дешифрует все указанные после ключа файлы. Каталоги помечаются как незашифрованные – все файлы, которые будут помещены в них впоследствии, шифроваться не будут
/S	Выполняет заданную операцию с каталогом *каталог* и всеми его подкаталогами, файлы при этом не обрабатываются
/A	Выполняет определенную ключом операцию как для каталогов, так и для отдельных файлов

Ключ	Описание
/I	Продолжает выполнение указанной операции даже после возникновения ошибочной ситуации. По умолчанию при появлении ошибки программа cipher
/F	Осуществляет принудительное шифрование всех файлов, указанных после ключа, даже если они уже зашифрованы. По умолчанию уже зашифрованные файлы не подвергаются вторичному шифрованию
/Q	Выдает только краткую информацию
/H	Отображает файлы, для которых установлены атрибуты *скрытый* (Hidden) и *системный* (System)
/K	Создает новый ключ шифрования файлов для пользователя, запустившего команду; при этом все другие ключи команды игнорируются

Параметр *путь* может быть маской, файлом или каталогом. Команда cipher без параметров выдает информацию о том, зашифрован ли данный каталог или файлы, находящиеся в нем. Если параметр *путь* присутствует, то имен файлов может быть несколько. Между собой параметры должны быть разделены пробелом.

Для того чтобы зашифровать каталог **Мои документы,** введите команду:

```
C:\cipher /E “Мои документы”
```

Для того чтобы зашифровать все файлы с расширением doc, введите команду:

```
C:\cipher /E /A *.doc
```

Шифрование файлов и каталогов

Поскольку шифрование и дешифрование выполняется автоматически, пользователь может работать с файлом так же, как и до установки его криптозащиты. Например, можно так же открыть текстовый

процессор Word, загрузить документ и отредактировать его, как и прежде. Все остальные пользователи, которые попытаются получить доступ к зашифрованному файлу, получат сообщение об ошибке доступа, поскольку они не владеют необходимым личным ключом, позволяющим им расшифровать файл.

Следует отметить, что пользователи (в данном случае администраторы) не должны шифровать файлы, находящиеся в системном каталоге, они необходимы для загрузки системы, в процессе которой ключи пользователя недоступны. Это сделает невозможным дешифрование загрузочных файлов, и система потеряет работоспособность. Проводник блокирует возможность возникновения такой ситуации, не позволяя шифровать файлы с атрибутом *системный*.

Шифрование информации задается в окне свойств файла или папки:

1. Укажите файл или папку, которую требуется зашифровать, нажмите правую кнопку мыши и выберите в контекстном меню команду **Свойства** (Properties).
2. В появившемся окне свойств на вкладке **Общие** (General) нажмите кнопку **Другие** (Advanced). Появится окно диалога **Дополнительные атрибуты** (Advanced Attributes) (рис. 32).
3. В группе **Атрибуты сжатия и шифрования** (Compress or Encrypt attributes) установите флажок **Шифровать содержимое для защиты данных** (Encrypt contents to secure data) и нажмите кнопку **ОК**.
4. Нажмите кнопку **ОК** в окне свойств зашифровываемого файла или папки. В появившемся окне диалога укажите режим шифрования.

При шифровании папки можно указать следующие режимы нового атрибута:

- **только к этой папке** (Apply changes to this folder);
- **к этой папке и всем вложенным папкам и файлам** (Apply changes to this folder, subfolders and files).

Дешифрование файлов и каталогов

1. Чтобы дешифровать файл или папку, на вкладке **Общие** окна свойств соответствующего объекта нажмите кнопку **Другие**.

2. В открывшемся окне диалога в группе **Атрибуты** сжатия и **шифрования** сбросьте флажок **Шифровать содержимое для защиты данных**.

Копирование, перемещение, переименование и уничтожение зашифрованных файлов и папок

Операции копирования, перемещения, переименования и уничтожения зашифрованных файлов и папок выполняются точно так же, как и с незашифрованными объектами. Однако следует помнить, что пункт назначения зашифрованной информации должен поддерживать шифрование (должен иметь файловую систему NTFS 5.0). В противном случае при копировании данные будут расшифрованы, и копия будет содержать открытую информацию.

Архивация зашифрованных файлов

Резервную копию зашифрованного файла можно создать с помощью простого копирования его на другой жесткий диск или с использованием утилиты архивации. Однако, как сказано в предыдущем разделе, простое копирование, например, на дискету или оптический диск может привести к тому, что резервная копия будет содержать открытые данные. То есть, если скопировать зашифрованный файл на раздел FAT или на дискету, копия будет не зашифрована и, следовательно, доступна для чтения любому пользователю.

Специализированная операция архивации не требует для ее выполнения доступа к открытым ключам пользователя – только к архивируемой информации. Поэтому для обеспечения безопасности конфиденциальных данных при создании резервных копий рекомендуется применять специальные утилиты архивации. В Windows 2000 для этих целей предназначена стандартная утилита архивации данных NTBackup.

В процессе архивации зашифрованные данные будут скопированы на указанный носитель без дешифрования. Целевой носитель может не поддерживать NTFS 5.0. Например, резервная копия зашифрованных файлов может быть создана на гибком диске.

СПИСОК ЛИТЕРАТУРЫ

1. Андреев А.Г. и др. Microsoft Windows 2000 Server. Русская версия/ Под общ ред. А.Н. Чекмарева и Д.Б. Вишнякова. СПб.: БХВ-Петербург, 2001.960 с.
2. Зубанов Ф. Microsoft Windows 2000. Планирование, развертывание, установка. М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 2001
3. Зубанов Ф. Windows NT –выбор «профи». – М.: Издательский отдел «Русская редакция» ТОО «Channel Trading Ltd.», 1996. 392с.
4. Титтел Э., Хадсон К., Стюарт Дж. М. NT Server 4.0. Сертификационный экзамен экстерном (экзамен 70-067). СПб: Издательство Питер, 1999.-400с.

ОГЛАВЛЕНИЕ