Лабораторная работа 1

Создание локальных учетных записей пользователей и групп

ЦЕЛЬ: Изучить методы создания и настройки одного из основного компонентов системы безопасности Windows 2000/XP – пользовательских учетных записей

1. Теоретические сведения

Создание учетных записей пользователей и групп занимает важное место в обеспечении безопасности Windows, поскольку, назначая им права доступа, администратор получает возможность ограничить пользователей в доступе к конфиденциальной информации, разрешить или запретить им выполнение в компьютере или сети определенного действия, 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. Для скрытия от посторонних глаз учетные записи, пароли и детали процесса регистрации необходимо реализовать следующие меры безопасности:

- создать отдельную учетную запись для каждого пользователя;
- отключить / удалить неиспользуемые учетные записи;
- сопоставить каждую группу безопасности и соответствующую учетную запись;
- для всех учетных записей подобрать нетривиальные пароли;
- обезопасить учетную запись администратора;
- выбрать политику работы с паролями, позволяющую гарантировать выбор/регулярное изменение паролей пользователей;
- обеспечить возможность восстановления утерянных паролей;
- использовать специальную программу для безопасной работы с паролями;
- отключить отображение начального экрана в процессе регистрации;
- перед началом процесса регистрации в системе потребовать, чтобы пользователи нажимали комбинацию клавиш Ctrl+Alt+Delete, а затем указывали свое имя и пароль;
- включить отображение экрана, информирующего пользователей о попытках несанкционированного доступа;
- ввести политику блокирования паролей, нивелирующую эффект программ по подбору паролей;
- в случае необходимости высшей степени безопасности обеспечить загрузку системы лишь в случае ввода специального пароля или применения других вспомогательных средств.

Создание и поддержка пользовательских учетных записей в Windows 2000 осуществляется с помощью следующих утилит: **Пользователи и пароли** (Users And Password), **Локальные пользователи и группы** (Local Users And Groups).

1.1. Утилита локальные пользователи и группы

Утилита л**окальные пользователи и группы** (Local Users and Groups) — это инструмент Microsoft Management Console (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 (member server). На контроллерах домена Windows 2000 инструмент **Локальные пользователи и группы** недоступен, поскольку все управление учетными записями и группами в домене выполняется с помощью утилиты **Active Directory — пользователи и компьютеры** (Active Directory Users and Computers). Запускать утилиты **Локальные пользователи и группы** может любой пользователь. Выполнять администрирование учетных записей могут только администраторы и члены группы **Опытные пользователи** (Power Users).

Окно изолированной утилиты **Локальные пользователи и группы** выглядит аналогично, показанному на рис. 1.

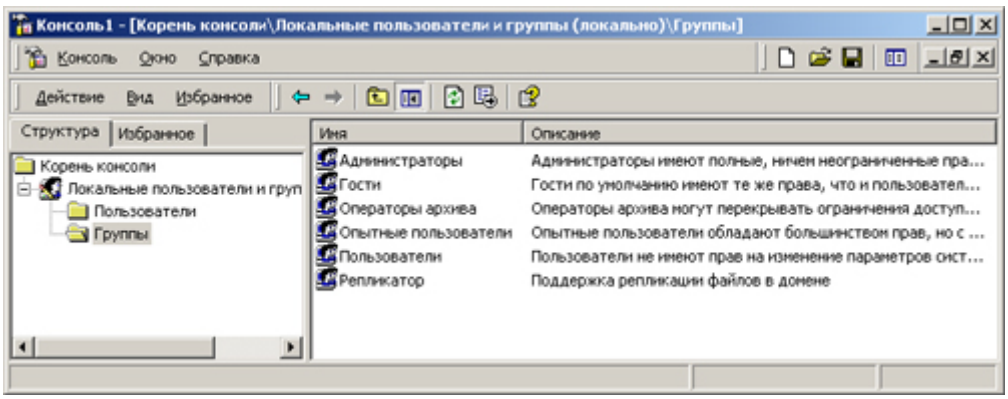

Рис. 1. Окно утилиты **Локальные пользователи и группы**

1.1. Папка Пользователи (Users)

Сразу после установки системы Windows 2000 (на рабочей станции или на сервере, 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 для регистрации 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.

1.2. 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.

- **Реплнкатор** (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.

1.3. Управление учетными записями

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

1.4. Создание учетной записи

Для создания учетной записи:

1. В утилите **Локальные пользователи и группы** установите указатель мыши на папку **Пользователи** и нажмите правую кнопку. В появившемся 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 пароль 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 действия пароля не ограничен** (Password never expires) и **Отключить учетную запись** (Account is disabled). См. рис. 2. и Табл. 2.

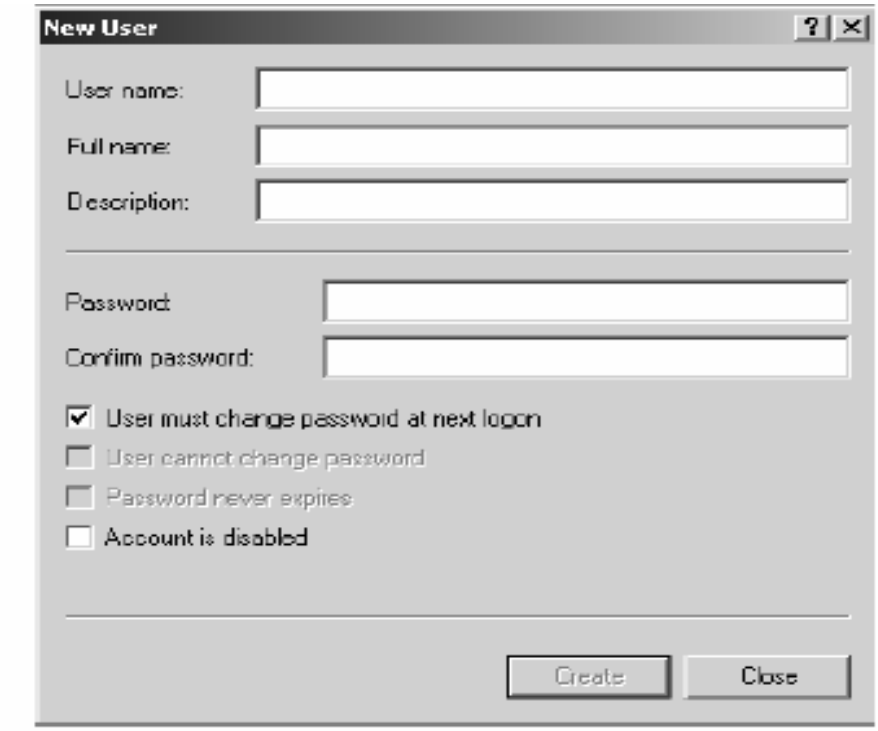

Рис. 2. Диалоговое окно новый пользователь (New User).

Таблица 2

Опции диалогового окна новый пользователь

Опция	Описание
User Name	Определяет имя пользователя для новой учетной записи. единственное обязательное поле. Имена пользователей не зависят от регистра.
Full Name	В этом поле можно указать более детальную информацию новом пользователе. Как правило, здесь задаются имя и ф пользователя. По умолчанию значение этого поля устанавливается равным значению поля User Name.
Description	Это поле служит для дополнительной информации. Как п здесь указываются наименование подразделения или конт данные.
Password	Здесь пользователю присваивается начальный пароль. Дл пароля может составлять до 14 символов, прописные и ст буквы считаются различными.
Confirm Password	Здесь следует второй раз ввести тот же самый пароль во избежание ошибки.
User Must Change Password at Next Logon	Если этот флажок установлен, пользователь обязан измен пароль при первом входе в систему. Это делается для повышения уровня безопасности. По умолчанию этот фла установлен.
User Cannot Change Password	Если этот флажок установлен, то пользователь не имеет п изменить пароль. Эта опция полезна для учетных записей подобных Guest, и других учетных записей, которыми пользуются несколько человек. По умолчанию этот флаж
	сброшен.
Password Newer Expires	Если этот флажок установлен, то срок действия пароля не ограничен во времени, даже если применяется политика смен паролей. Например, эта опция пригодна для служебных учетн записей. По умолчанию флажок сброшен.
Account Is Disabled	Если этот флажок установлен, под данной учетной записью нельзя войти в систему. Например, можно установить этот флажок для шаблонов учетной записи или для учетных запис зарезервированных для будущего применения. Таким образом можно избежать ослабления защиты. По умолчанию флажок сброшен.

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** (Close).

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

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

Имя пользователя не может состоять целиком из точек и пробелов.

Администраторы обозначают пользователей и группы именами, но система оперирует с уникальными идентификаторами системы защиты (Security Identifier, SID). SID генерируется при создании учетной записи; если удалить учетную запись, а потом создать новую с тем же именем, права старой учетной записи не перейдут к новой по одной простой причине – идентификаторы этих записей будут разными.

Идентификатор имеет формат S-R-A-S-S-S-S (табл. 1).

Таблица 1.

Структура идентификатора системы защиты.

Раздел	Название	Комментарий
S	SID	Признак идентификатора системы защиты.
R	Версия	Номер версии.
A	Распорядитель	48-разрядный идентификатор распорядителя системы защиты – например, домена Windows NT, создавшего этот идентификатор.
S	Владелец	Число, идентифицирующее владельца идентификатора.

В Windows существует два типа SID: создаваемые и встроенные. Первые создаются ОС и администраторами (естественно, средствами ОС). Формат этих идентификаторов аналогичен описанному выше, иной смысл лишь у поля «владелец». Рассмотрим, например, идентификатор S-1-5-21-498661181-976881882-12541761-1009 (табл. 2).

Таблица 2.

Содержимое идентификатора системы защиты.

Раздел	Комментарий
S	Признак идентификатора системы защиты
1	Версия 1.
5	Идентификатор распорядителя системы защиты (5-NT).
21	Первый владелец – домен или рабочая группа.
397661181-626881882-18441761	Второй, третий и четвертый владельцы – эти значения уникально идентифицируют домен и рабочую группа группу.
1009	Последнее поле, значение которого начинается с 1001, идентифицирует учетную запись пользователя. Это значение автоматически увеличивается при создании каждой новой учетной записи.

1.5. Изменение и удаление учетных записей

Изменять, переименовывать и удалять учетные записи можно с помощью 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, SID), она сохраняет и все свои свойства, например, описание, полное имя пароля, членство в группах и т. д.

1.6. 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. Оно может содержать до 256 символов в верхнем и нижнем регистрах. В имени группы запрещено применение символа обратного слэша (\).

1.7. 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 добавитв 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.

1.8. 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. Все настройки, выполняемые самим пользователем, автоматически сохраняются в файле, путь к которому выглядит следующим образом: *Имя_устройства\корневой_каталог\ProF\\e$*. Как правило, корневым является каталог \winnt.
- ***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.

1.9. 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).

Внимание

Не все настройки локального профиля пользователя входят (копируются) в его перемещаемый профиль!

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.

1.10. Настройки, хранящиеся в профиле пользователя

Профиль пользователя хранит настройки конфигурации и параметры, индивидуально назначаемые каждому пользователю и полностью определяющие его рабочую среду (табл. 1).

Таблица 1.

Настройки профиля пользователя

Объект	Соответствующие 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 операционной системе Windows 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

1.11. Структура профиля пользователя

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.**

1.11.1. 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. 2 показана структура папок ***локального*** профиля пользователя. В этих папках, в частности, хранятся ссылки на различные объекты рабочего стола.

В табл. 2 перечислены подпапки, находящиеся внутри папки локального профиля пользователя, и описано их содержимое.

Таблица 2.

Содержимое папки локального профиля пользователя

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 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
SendTo	Ярлыки объектов, куда могут посылаться документы
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 ярлыки
Шаблоны (Templates)	Ярлыки шаблонов

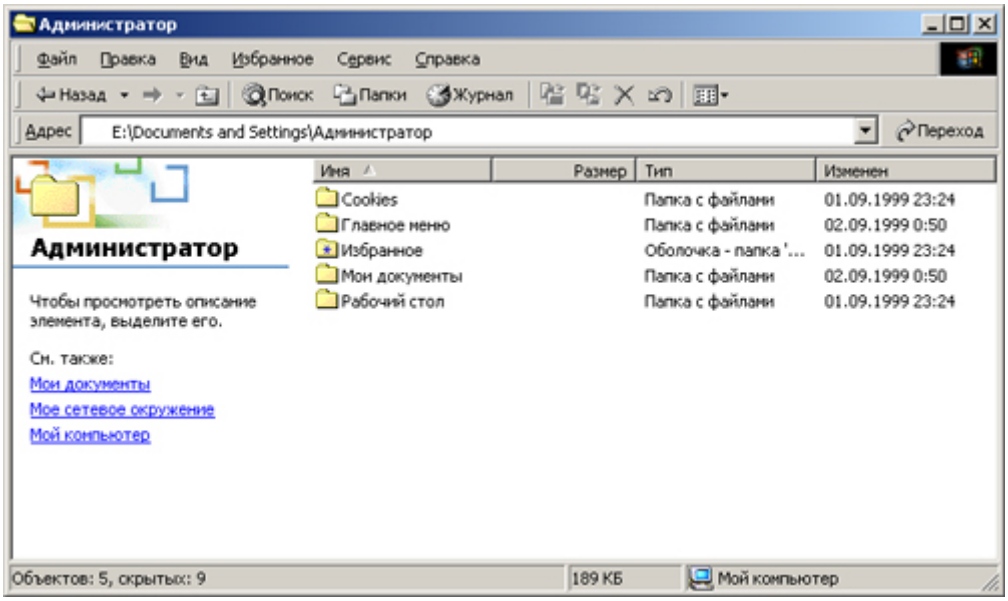

Рис. 2. Структура подпапок профиля пользователя

1.11.2. 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.**

1.12. 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 им 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 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. 2). Он нужен для обеспечения отказоустойчивости, позволяя Windows 2000 восстанавливать профиль пользователя в случае сбоя при модификации содержимого файла **NTuser.dat.**

1.13. 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.

Внимание.

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 Active Directory - пользователи и компьютеры (Active Directory Users and Computers), поскольку основная информация о пользователях домена хранится в каталоге. В остальном логика управления профилями остается неизменной: перемещаемый профиль хранится в указанной папке на некотором общем сетевом ресурсе, а в случае его недоступности используется кэшированная копия с локального компьютера.

С помощью утилиты Локальные пользователи и группы можно указать имя сервера, где будет храниться заранее созданный перемещаемый профиль пользователя. Затем 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 профиля на сервер. 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 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.*

1.14. 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 **Active Directory — пользователи и компьютеры).** Перейдите на вкладку **Профиль** и добавьте путь к профилю пользователя (рис. 3).

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 следует 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 не 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.

1.14.1. Копирование профиля пользователя на сервер

Для того чтобы сделать определенный профиль доступным для нескольких пользователей, скопируйте его, на сервер с помощью вкладки **Профили пользователей** окна **Система,** вызываемого из панели управления. Место, куда

скопирован профиль, должно совпадать с путем профиля, указанным в учетных записях пользователей.

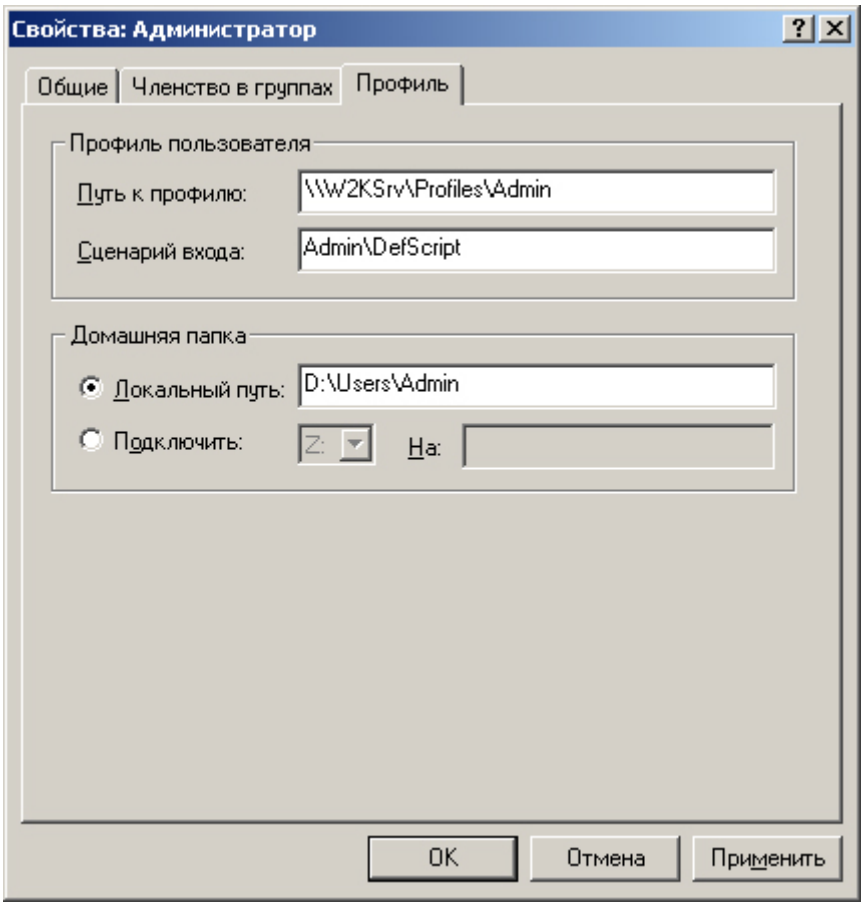

Рис. 3. Вкладка **Профиль** (Profile) окна свойств учетной записи

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. 4 показан пример окна **Свойства системы** со списком созданных на компьютере профилей пользователя.

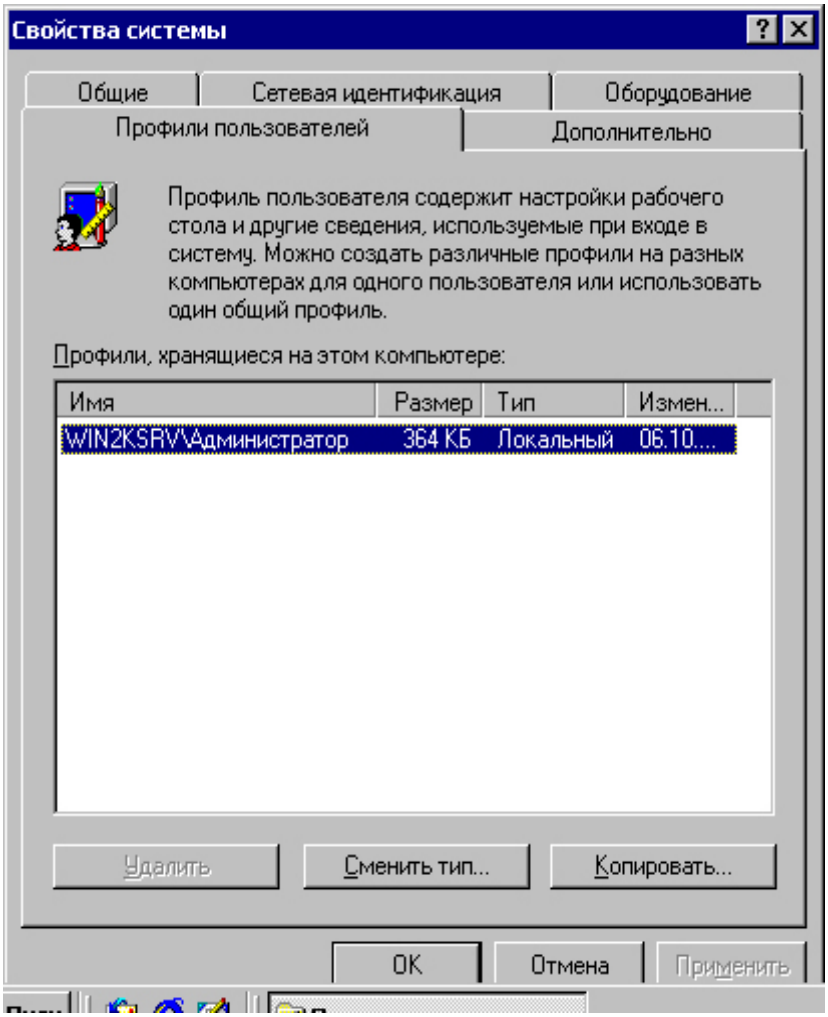

Рис. 4. Окно **Свойства системы** (System Properties) со списком созданных на компьютере профилей пользователя

1.14.2. Добавление пользователей и групп к списку разрешений перемещаемого профиля пользователя

С помощью окна **Система** вместе с профилем пользователя копируются и 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 компьютере** выберите интересующий вас профиль и нажмите кнопку **Копировать.** Появится окно диалога **Копирование профиля** (Copy To) (рис. 5). 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.

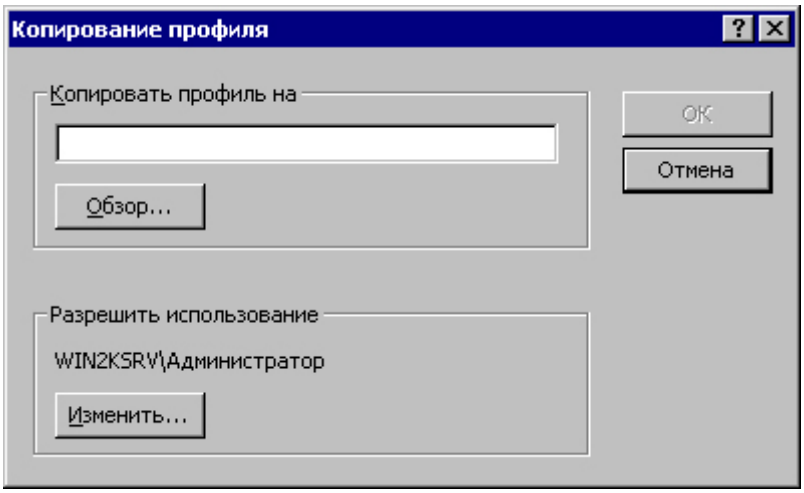

Рис. 5. Окно диалога **Копирование профиля** (Copy To)

1.15. Работа пользователей с различными конфигурациями оборудования

Следует помнить, что профили могут применяться на компьютерах, отличающихся по конфигурации оборудования, особенно типами мониторов и видеоадаптеров.

Профиль пользователя может определять положение и размер окон, поэтому тип оборудования экрана в значительной степени влияет на качество работы профиля. Например, параметры окна, выводимого на экране типа Super VGA, могут быть неверны при выводе того же изображения на экране с типом VGA. Для предотвращения подобных проблем:

- Создавайте и редактируйте профиль пользователя на компьютере, тип экрана которого совпадает с типом экрана компьютера пользователя;
- При создании обязательного профиля для нескольких пользователей создавайте один профиль для группы пользователей только в случае, если все члены группы работают на компьютерах с одинаковым типом экранов.

1.16. Удаление профиля пользователя

Если вы больше не хотите использовать перемещаемый или обязательный профиль, назначенный пользователям, с помощью оснастки **Локальные пользователи и группы** удалите путь к нему в учетных записях соответствующих пользователей. Сам профиль пользователя, находящийся на сервере, можно удалить с помощью кнопки **Удалить** на вкладке **Профили пользователей** окна **Система.**

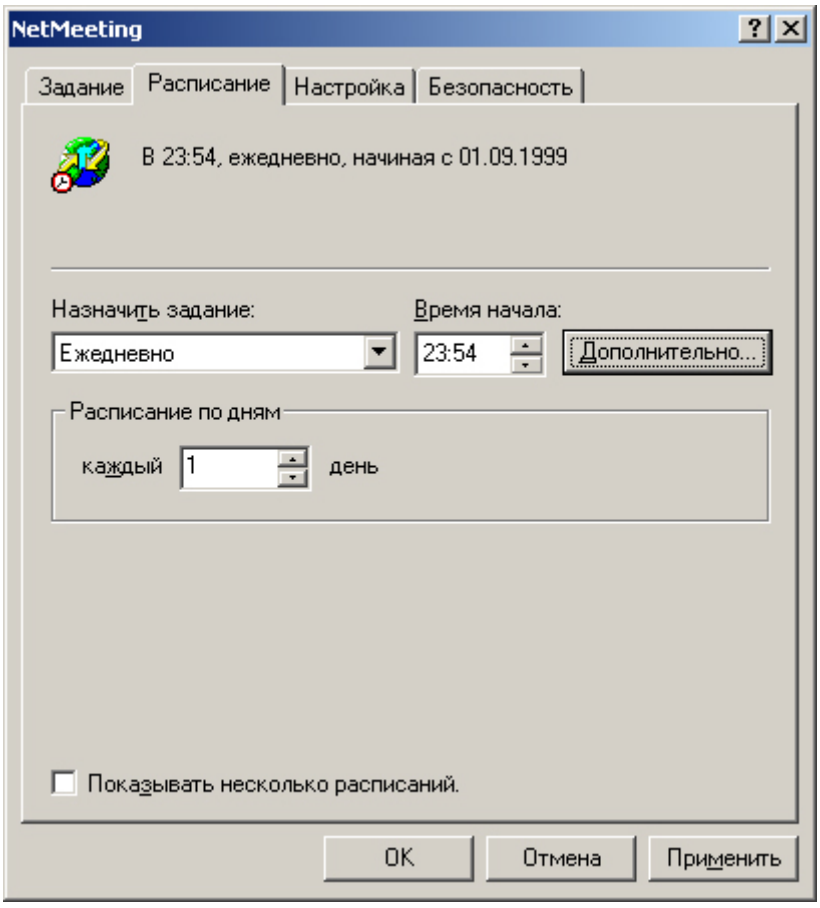

Рис. 7. Вкладка **Расписание** (Schedule) для запланированного запуска программы NetMeeting .

2. Контрольные вопросы

1. Перечислите основные меры безопасности, которые обязан реализовать администратор.
2. Назначение утилиты локальные пользователи и группы.
3. Перечислите основные свойства встроенной учетной записи –Администратор.
4. Перечислите основные свойства встроенной учетной записи – Гость.
5. Сколько встроенных групп и каких содержит папка **Группы.**
6. Раскройте структуру идентификатора системы защиты.
7. Какие средства Windows 2000 предназначены для управления средой пользователя.
8. Для чего необходима информация локального профиля пользователя.
9. В каком файле содержатся настройки конфигурации, хранящиеся в реестре Windows 2000
10. Что содержит папка ***локального*** профиля пользователя.
11. Где хранятся файл **NTuser.d**at и файл журнала транзакций с именем **NTuser.dat.LOG**.
12. Перечислите способы создания перемещаемых профилей пользователя.
13. Назначение обязательного профиля пользователя.

4. Порядок выполнения

1. Ответить на контрольные вопросы.
2. Выполнить задания.
3. Защитить полученные результаты.

Задания:

1. Введите 8 новых пользователей. Для каждого пользователя задайте **User Name, Full Name, Description и Password, Confirm Password** на свой выбор. Заблокируйте одну из учетных записей. Установите различное время действие паролей.
2. Создайте 4 различные группы. Включите в каждую группу по два пользователя.
3. Используя Windows Explorer, создайте 8 папок в своей директории.
4. Укажите для каждого пользователя доступ к двум личным папкам.
5. Задайте для каждого пользователя различную конфигурацию оборудования.

6. Создать несколько типов профилей и назначить их определенным группам пользователей.