# Лабораторная работа № 10

**УЧЁТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ**

# (2 часа)

**ЦЕЛЬ РАБОТЫ:** изучение возможностей управления учётными записями пользователей в ОС Windows Server 2003

# ЗАДАЧИ РАБОТЫ

1. Изучить свойства учетных записей пользователей как средства назначе- ния разрешений, сценариев регистрации, профилей и домашних каталогов.
2. Научиться создавать учетные записи пользователей и групп пользовате- лей в ОС Windows Server 2003.

# ПЕРЕЧЕНЬ ОБЕСПЕЧИВАЮЩИХ СРЕДСТВ

1. ПК.
2. Программное обеспечение: Oracle VirtualBox, ОС Windows Server 2003. 3.Учебно-методическая литература.

# ОБЩИЕ ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Пользовательская учетная запись содержит имя и пароль для регистрации на локальном компьютере или в домене. В Active Directory (AD) учетная запись пользователя может также содержать дополнительную информацию, такую как полное имя пользователя, адрес электронной почты, номер телефона, отдел и физический адрес. Кроме того, учетная запись пользователя служит средством для назначения разрешений, сценариев регистрации, профилей и домашних ка- талогов.

В Windows Server 2003 определены пользовательские учетные записи двух типов: доменные учетные записи и локальные учетные записи.

*Доменные учетные записи* определены в Active Directory. Посредст- вом системы однократного ввода пароля такие учетные записи могут обращать- ся к ресурсам во всем домене. Они создаются в консоли «Active Directory — пользователи и компьютеры».

*Локальные учетные записи* определены на локальном компьютере, имеют доступ только к его ресурсам и должны аутентифицироваться, прежде чем получат доступ к сетевым ресурсам. Локальные учетные записи пользова- телей создают в оснастке «Локальные пользователи и группы».

Локальные учетные записи пользователей и групп хранятся только на ря- довых серверах и рабочих станциях. На первом контроллере домена они пере- мещаются в Active Directory и преобразуются в доменные учетные записи.

Все учетные записи пользователей распознаются по имени для входа в систему. В Windows Server 2003 оно состоит из двух частей:

* «имя пользователя» — текстовое имя учетной записи;
* «домен или рабочая группа», в которых находится учетная запись. Например: для пользователя mask, учетная запись которого создана в до-

мене is4.local, полное имя для входа в Windows Server 2003 выглядит так — [mask@is4.local.](mailto:mask@is4.local) Имя для предыдущих версий Windows — is4\ mask. При работе с Active Directory иногда требуется полное имя домена пользователя, состоя- щее из DNS-имени домена в сочетании с именами контейнера и группы. У пользователя is4.local \Users\ mask, is4.local — DNS-имя домена, Users - имя контейнера, а mask — имя пользователя.

С учетной записью пользователя могут сопоставляться пароль и открытый сертификат. В открытом сертификате сочетаются открытый и закрытый ключ для идентификации пользователя. Вход в систему по паролю проходит инте- рактивно. При входе в систему с открытым сертификатом используются смарт- карта и считывающее устройство.

Хотя для назначения привилегий и разрешений в Windows Server 2003 применяются имена пользователей, ключевым идентификатором учетной запи- си является генерируемый при создании уникальный идентификатор безопас- ности (SID). Он состоит из идентификатора безопасности домена и уникально- го относительного идентификатора, который был выделен хозяином относи- тельных идентификаторов.

С помощью SID, ОС Windows Server 2003 способна отслеживать учетные записи независимо от имен пользователей. Благодаря наличию SID вы вправе изменять имена пользователей и удалять учетные записи, не беспокоясь, что кто-то получит доступ к ресурсам, создав учетную запись с тем же именем. Ко- гда вы меняете имя пользователя, Windows Server 2003 сопоставляет прежний SID с новым именем. Когда вы удаляете учетную запись, Windows Server 2003 считает, что конкретный SID больше недействителен**.** Если вы затем создадите учетную запись с тем же именем, она не получит привилегий предыдущей за- писи, так как у нее иной SID.

Помимо учетных записей пользователей в Windows Server 2003 использу- ются группы, позволяющие автоматически предоставлять разрешения схожим типам пользователей и упростить администрирование учетных записей. Если пользователь — член группы, которая вправе обращаться к ресурсу, то он тоже может к нему обратиться. Чтобы предоставить пользователю доступ к нужным ресурсам, вы просто включаете его в подходящую группу. Поскольку в разных доменах Active Directory могут быть группы с одинаковыми именами, на груп- пы часто ссылаются по полному имени — домен\имя\_группы*.*

В Windows Server 2003 используются группы трех типов:

* *локальные группы* определяются и используются только на локальном компьютере, создаются в оснастке «Локальные пользователи и группы»;
* *группы безопасности* располагают дескрипторами защиты и определяют- ся в доменах посредством консоли «Active Directory — пользователи и компью- теры». Это те группы, для которых можно назначать права и разрешения. Права определяют, какая деятельность разрешается в домене члену подобной группы (пользователю или компьютеру), а разрешения определяют, к каким объектам в

сети они будут иметь доступ. Группы безопасности можно использовать и для рассылки e-mail сообщений многим пользователям. Сообщение отсылается лишь один раз, но при этом его получают все члены группы. Для этого, впро- чем, в сети должен быть установлен продукт Microsoft Exchange Server 2003. В этом случае группы безопасности ведут себя так же, как группы распростране- ния;

* *группы распространения* используются как списки рассылки электрон- ной почты, не имеют дескрипторов безопасности и определяются в доменах по- средством консоли «Active Directory — пользователи и компьютеры». Эти группы предназначены только для рассылки пользователям сообщений элек- тронной почты. Для них не определяются права доступа к сетевым объектам.

Группы безопасности имеют все свойства групп распространения, но не наоборот. Но дело в том, что некоторые приложения могут работать только с ними, а не с группами безопасности.

У групп возможны разные области действия *—* локальная доменная, встро- енная локальная, глобальная и универсальная. От этого зависит, в какой части сети они действительны.

*Локальные доменные группы* предоставляют разрешения в одном домене, В состав локальных доменных групп входят лишь учетные записи (и пользова- телей, и компьютеров) и группы из домена, в котором они определены.

*Встроенные локальные группы* обладают особыми разрешениями в ло- кальном домене. Для простоты их часто также называют локальными домен- ными группами, но в отличие от обычных групп, встроенные локальные группы нельзя создать или удалить — можно лишь изменить их состав. Как правило, говоря о локальных доменных группах, имеется в виду и обычные, и встроен- ные локальные группы, если не указано обратное.

*Глобальные группы* используются для назначения разрешений на доступ к объектам в любом домене дерева или леса. В глобальную группу входят только учетные записи и группы из домена, в котором они определены.

*Универсальные группы* управляют разрешениями во всем дереве или лесе; в них входят учетные записи и группы из любого домена в дереве или лесе до- мена. Универсальные группы доступны только в Active Directory в основном режиме Windows 2000 или в режиме Windows Server 2003.

Универсальные группы очень полезны на больших предприятиях, имею- щих несколько доменов. Состав универсальных групп не должен часто менять- ся, так как любое изменение надо реплицировать во все глобальные каталоги в дереве или лесе. Чтобы уменьшить количество изменений, включайте в универ- сальную группу только группы, а не сами учетные записи.

В Windows Server 2003 учетные записи групп, как и учетные записи поль- зователей, различаются по уникальным идентификаторам безопасности. Это значит, что нельзя удалить учетную запись группы, а затем создать группу с тем же именем, чтобы у нее появились прежние разрешения и привилегии. У новой группы будет новый SID, и все разрешения и привилегии старой группы будут утеряны.

Для каждого сеанса пользователя в системе Windows Server 2003 создает маркер безопасности, содержащий идентификатор учетной записи пользователя и SID всех групп безопасности, к которым относится пользователь. Размер мар- кера растет по мере того, как пользователь добавляется в новые группы безо- пасности. Это приводит к следующим последствиям:

* чтобы пользователь вошел в систему, маркер безопасности должен быть передан процессу входа в систему. Поэтому по мере увеличения членства поль- зователя в группах безопасности процесс входа требует все больше времени;
* чтобы выяснить разрешения доступа, маркер безопасности пересылается на каждый компьютер, к которому обращается пользователь. Поэтому чем больше маркер безопасности, тем выше сетевой трафик.

Сведения о членстве в группах распространения не передаются в маркере безопасности, поэтому состав этих групп не влияет на размер маркера.

# ЗАДАНИЕ

1. Создать учётную запись пользователя.
2. Изучить свойства созданной учётной записи.
3. Создать группу безопасности и группу распространения, включить учётную запись пользователя в эти группы.
4. Создать шаблон учетной записи.

# ТРЕБОВАНИЯ К ЗАЧЕТУ

1. К зачету необходимо предоставить результаты выполненной работы.
2. Отчет с подробным описанием выполненных работ.
3. Подготовить ответы на вопросы.

# ТЕХНОЛОГИЯ ВЫПОЛНЕНИЯ РАБОТЫ

## Создание доменной учетной записи

1. На сервере запустить консоль «Active Directory — пользователи и ком- пьютеры».
2. Перед созданием учетной записи пользователя необходимо создать но- вое подразделение. Для этого в левом окне консоли щелкнуть правой кнопкой мыши по значку домена и из контекстного меню выбрать «Создать» - «Подраз- деление».
3. В появившемся диалоговом окне ввести имя подразделения, например:

«*student*».

1. После создания подразделения приступить к созданию учётной записи пользователя. Для этого требуется щелкнуть правой кнопкой мыши по создан- ному подразделению «*student*» и из контекстного меню выбрать «Создать» -

«Пользователь».

1. В диалоговом окне «Новый объект - Пользователь». Заполнить пункты

«Имя» и «Фамилия».

1. В поле «Имя входа пользователя» ввести «*User1*». Это же регистрацион- ное имя будет автоматически введено и в поле «Имя входа в систему пользова-

теля (пред-Windows 2000)». Данное значение можно изменить вручную, но это не рекомендуется. Нажмите «Далее».

Рекомендуется избегать использования в регистрационном имени символы кириллицы, поскольку не на каждом компьютере можно переключиться на рус- скую раскладку в ходе регистрации (рис.10.1).

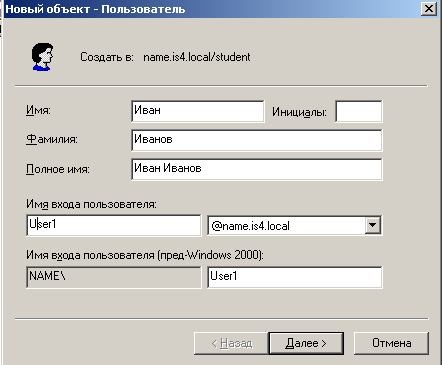


Рис. 10.1. Заполненное диалоговое окно «Новый объект - Пользователь».

1. Заполните поля «Пароль» и «Подтверждение».

При этом необходимо придумать и ввести сложный пароль, удовлетво- ряющий следующим минимальным требованиям:

* пароль не может содержать имя учетной записи пользователя или ка- кую-либо его часть;
* пароль должен состоять не менее чем из семи символов;
* в пароле должны присутствовать символы трех категорий из числа сле- дующих четырех: прописные буквы английского алфавита от A до Z, строчные буквы английского алфавита от a до z, десятичные цифры (от 0 до 9), неалфа- витные символы (например, !, $, #, %).

1. При необходимости установить флажок «Требовать смену пароля при следующем входе в систему».
2. После проверки информации о новом пользователе завершить создание учетной записи нового пользователя.

## Изучение свойств созданной учётной записи.

1. Открыть свойства созданной учетной записи пользователя.
2. Изучить все вкладки.
3. Заполнить вкладки «Общие», «Адрес», «Организация».
4. Сделать учетную запись членом группы «Администраторы домена». Для этого следует на вкладке «Член групп» выполнить команду «Добавить».
5. В появившемся диалоговом окне выполнить команды «Дополнительно»

- «Поиск».

1. Из результатов поиска выбрать группу «Администраторы домена».
2. Задать основную группу - «Администраторы домена»
3. Исключить учетную запись из группы «Пользователи домена».

## Включение учётной записи пользователя в созданные группы.

Для создания новой группы требуется выполнить следующее:

1. Щелкнуть правой кнопкой мыши по подразделению «*student*» и из кон- текстного меню выбрать «Создать» - «Группа».
2. В появившемся диалоговом окне заполнить поля «Имя группы» и «Имя группы (пред-Windows 2000)» в соответствие с правилами, например: «*security*» (рис.10.2).
3. Установить область действия «Глобальная» и «Тип группы» - «Группа безопасности».

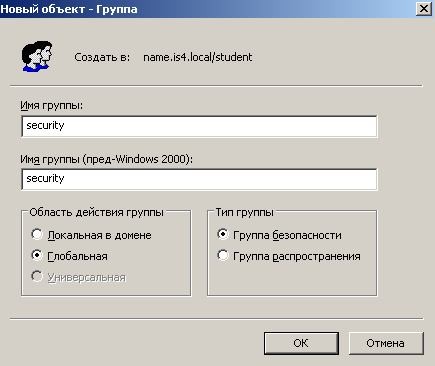


Рис. 10.2. Диалоговое окно «Новый объект - Группа».

1. Создать группу «*extending*». Установив «Область действия группы» -

«Универсальная», «Тип группы» - «Группа распространения» (рис. 10.3).

1. Включить вашу учетную запись в созданные группы.

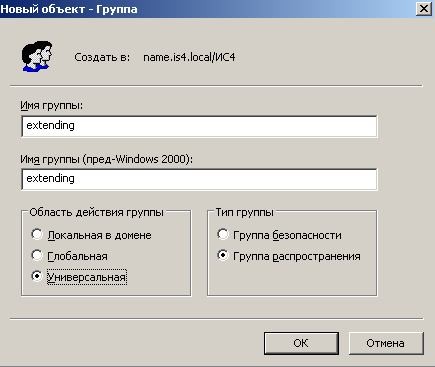


Рис. 10.3. Создание группы «extending».

## Создание шаблона

Последовательность действий по созданию шаблона состоит из следую- щих этапов:

1. Запустить консоль «Active Directory — пользователи и компьютеры» и создать пользователя с именем *«mask»* (рис.10.4).

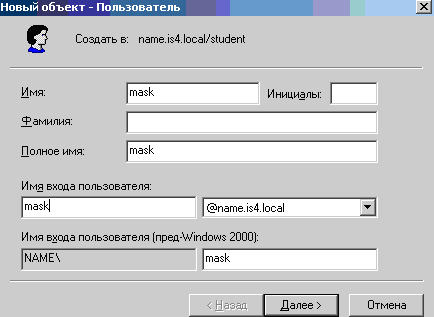


Рис. 10.4. Создание пользователя с именем «mask»

1. В окне свойств вновь созданной записи заполнить все необходимые поля на вкладках «Адрес» и «Организация».
2. Используя вкладку «Учетная запись» установить время входа для поль- зователя с понедельника по субботу с 8:00 до 18:00 (рис.10.5).

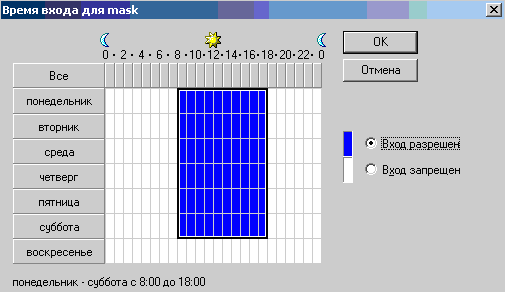


Рис. 10.5. Окно редактирования времени входа для пользователя

1. Далее нужно щелкнуть по созданной записи правой кнопкой мыши и из контекстного меню выбрать команду «Отключить учетную запись» (рис.10.6).



Рис. 10.6. Отключение учетной записи

## Создание учетной записи по шаблону

1. Щелкнуть по шаблону *«mask»* правой кнопкой мыши и из контекстного меню выбрать команду «Копировать».
2. В появившемся окне ввести регистрационное имя *«mask1»*, в качестве имени и фамилии тоже *«mask1».*
3. Задать пароль для первого входа в систему и снять флажок «Отключить учетную запись».

# КОНТРОЛЬНЫЕ ВОПРОСЫ

1. Что содержит пользовательская учетная запись?
2. Какие типы учетных записей определены в Windows Server 2003?
3. Из каких частей состоит имя для входа в систему Windows Server 2003?
4. Что такое SID?
5. Для чего создаются группы пользователей?
6. Какие три типа групп используются в ОС Windows Server 2003?
7. Можно ли удалив учетную запись группы, создать заново группу с та- ким же именем с тем, чтобы у нее появились прежние разрешения и привиле- гии? Ответ объяснить.
8. Что содержит маркер безопасности, который создает ОС Windows Server 2003 для каждого сеанса пользователя?
9. Объясните, почему, чем больше маркер безопасности, тем выше сетевой трафик.