Создание учетных записей пользователей в Active Directory

Введение

Основополагающим компонентом доменных служб в каждой организации являются принципалы безопасности (оригинальное название - Security Principal), которые предоставляют пользователей, группы или компьютеры, которым требуется доступ к определенным ресурсам в сети. Именно таким объектам, как принципалам безопасности можно предоставлять разрешения доступа к ресурсам в сети, причем каждому принципалу во время создания объекта присваивается уникальный идентификатор безопасности (SID), который состоит из двух частей. **Идентификатором безопасности SID** называется числовое представление, которое уникально идентифицирует принципал безопасности. Первая часть такого идентификатора представляет собой **идентификатор домена**. Ввиду того, что принципалы безопасности расположены в одном домене, всем таким объектам присваивается один и тот же идентификатор домена. Второй частью SID является **относительный идентификатор (RID)**, который используется для уникальной идентификации принципала безопасности по отношению к ведомству, которое выдает SID.
Несмотря на то, что планирование и развертывание инфраструктуры доменных служб в большинстве организаций выполняется лишь один раз и в большинство объектов изменения вносятся очень редко, к важному исключению из этого правила можно отнести принципалы безопасности, которые необходимо периодически добавлять, изменять, а также удалять. Одним из основополагающих компонента идентификации являются учетные записи пользователей. По сути, учетные записи пользователей представляют собой физические объекты, в основном людей, которые являются сотрудниками вашей организации, но бывают исключения, когда учетные записи пользователей создаются для некоторых приложений в качестве служб. Учетные записи пользователей играют важнейшую роль в администрировании предприятии. К таким ролям можно отнести:

- **Удостоверение личности пользователей**, так как созданная учетная запись позволяет входить на компьютеры и в домены именно с теми данными, подлинность которых проверяет домен;
- **Разрешения доступа к ресурсам домена**, которые назначаются пользователю для предоставления доступа к доменным ресурсам на основании явных разрешений.

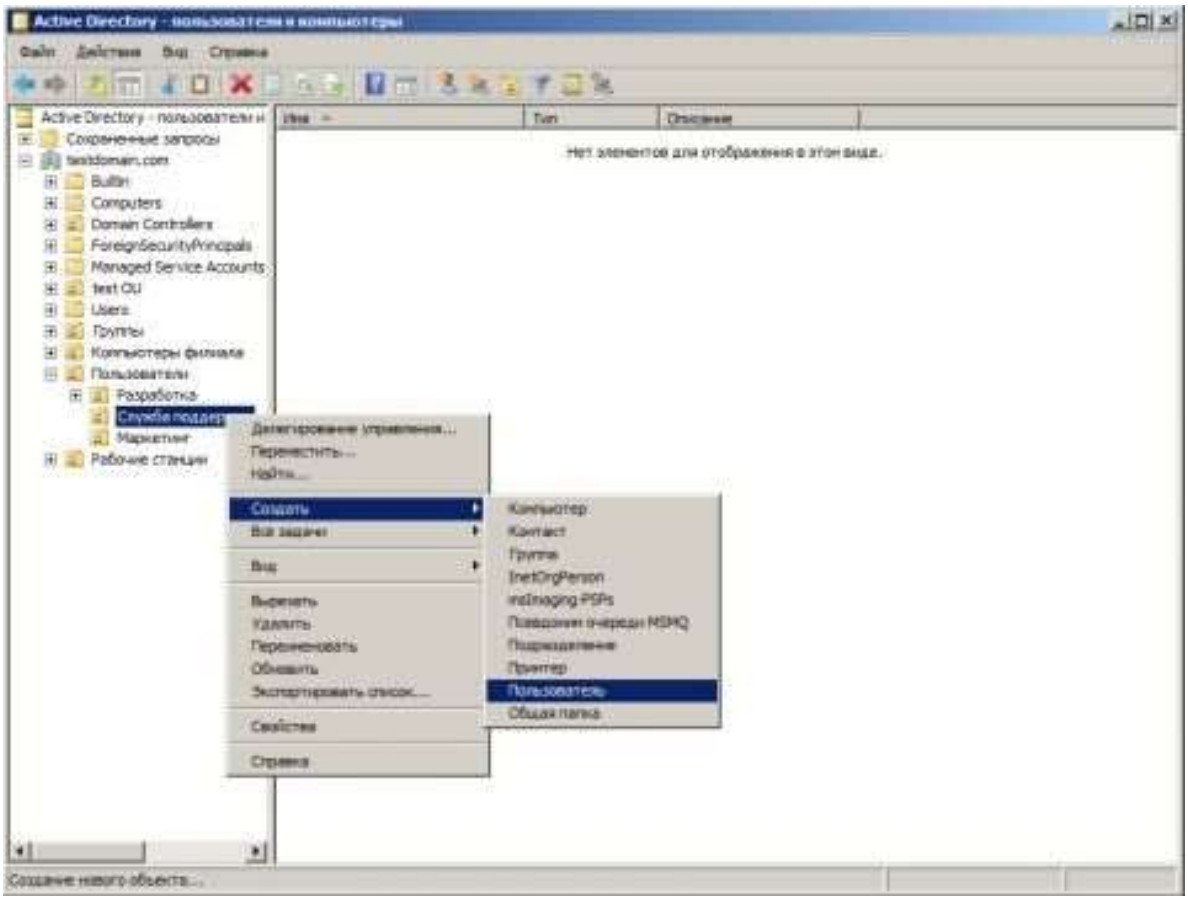
Объекты учетных записей пользователей можно отнести к самым распространенным объектам в Active Directory. Именно пользовательским учетным записям администраторы обязаны уделять особое внимание, так как пользователям свойственно приходить работать в организацию, перемещаться между отделами и офисами, жениться, выходить замуж, разводиться и даже увольняться из компании. Такие объекты представляют собой набор атрибутов, причем только одна пользовательская учетная запись может содержать свыше 250 различных атрибутов, что в несколько раз превышает количество атрибутов на рабочих станциях и компьютеров, работающих под операционной системой Linux. Во время создания учетной записи пользователя создается ограниченный набор атрибутов, а уже потом вы можете добавлять такие пользовательские учетные данные как организационные сведения, адреса проживания пользователей, телефонные номера и многое другое. Поэтому важно обратить внимание на то, что одни атрибуты являются **обязательными**, а остальные – **опциональными**. В этой статье я расскажу о ключевых методах создания пользовательских учетных записей, о некоторых опциональных атрибутах, а также будут описаны средства, позволяющие автоматизировать рутинные действия, связанные с созданием учетных записей пользователей.

Создание пользователей при помощи оснастки «Active Directory – пользователи и компьютеры»

В подавляющем большинстве случаев системные администраторы для создания основных принципалов безопасности предпочитают использовать оснастку **«Active Directory – пользователи и компьютеры»**, которая добавляется в папку **«Администрирование»** сразу после установки роли **«Доменные службы Active Directory»** и повышения сервера до контролера домена. Этот метод является наиболее удобным, так как для создания принципалов безопасности используется графический пользовательский интерфейс и мастер создания учетных записей пользователя очень прост в применении. К недостатку данного метода можно отнести тот момент, что при создании учетной записи пользователя вы не можете сразу задать большинство атрибутов, и вам придется добавлять необходимые атрибуты путем редактирования учетной записи. Для того чтобы создать пользовательскую учетную запись, выполните следующие действия:

1. Откройте оснастку **«Active Directory – пользователи и компьютеры»**. Для этого вам нужно открыть панель управления, в ней открыть раздел **«Система и безопасность»**, затем **«Администрирование»** и в появившемся окне открыть оснастку **«Active Directory – пользователи и компьютеры»**. Также вы можете воспользоваться комбинацией клавиш +R для открытия диалога **«Выполнить»** и в диалоговом окне **«Выполнить»**, в поле **«Открыть»** ввести *dsa.msc*, а затем нажать на кнопку **«ОК»**;

2. В дереве оснастки, разверните узел своего домена и перейдите к подразделению, в котором будет создаваться пользовательская учетная запись. Для создания пользовательских учетных записей рекомендуется создавать дополнительные подразделения, после чего добавлять учетные записи пользователей в подразделения, отличающиеся от стандартного подразделения Users. Щелкните на этом подразделении правой кнопкой мыши и из контекстного меню выберите команду **«Создать»**, а затем **«Пользователь»**, как показано на следующей иллюстрации:



Увеличить рисунок

Рис. 1. Оснастки «Active Directory – пользователи и компьютеры» и создание нового пользователя

3. В появившемся диалоговом окне **«Новый объект - Пользователь»** введите следующую информацию:
   - В поле **«Имя»** введите имя пользователя;
   - В поле **«Инициалы»** введите его инициалы (чаще всего инициалы не используются);
   - В поле **«Фамилия»** введите фамилию создаваемого пользователя;
   - Поле **«Полное имя»** используется для создания таких атрибутов создаваемого объекта, как основное имя (Common Name) **CN** и отображения свойств имени. Это поле должно быть уникальным во всем домене, и заполняется автоматически, а изменять его стоит лишь в случае необходимости;
   - Поле **«Имя входа пользователя»** является обязательным и предназначено для имени входа пользователя в домен. Здесь вам нужно ввести имя пользователя и из раскрывающегося списка выбрать суффикс UPN, который будет расположен после символа @;
   - Поле **«Имя входа пользователя (Пред-Windows 2000)»** предназначено для имени входа для систем предшествующих операционной системе Windows 2000. В последние годы в организациях все реже встречаются обладатели таких систем, но поле обязательно, так как некоторое программное обеспечение для идентификации пользователей использует именно этот атрибут;

   После того как заполните все требуемые поля, нажмите на кнопку **«Далее»**:

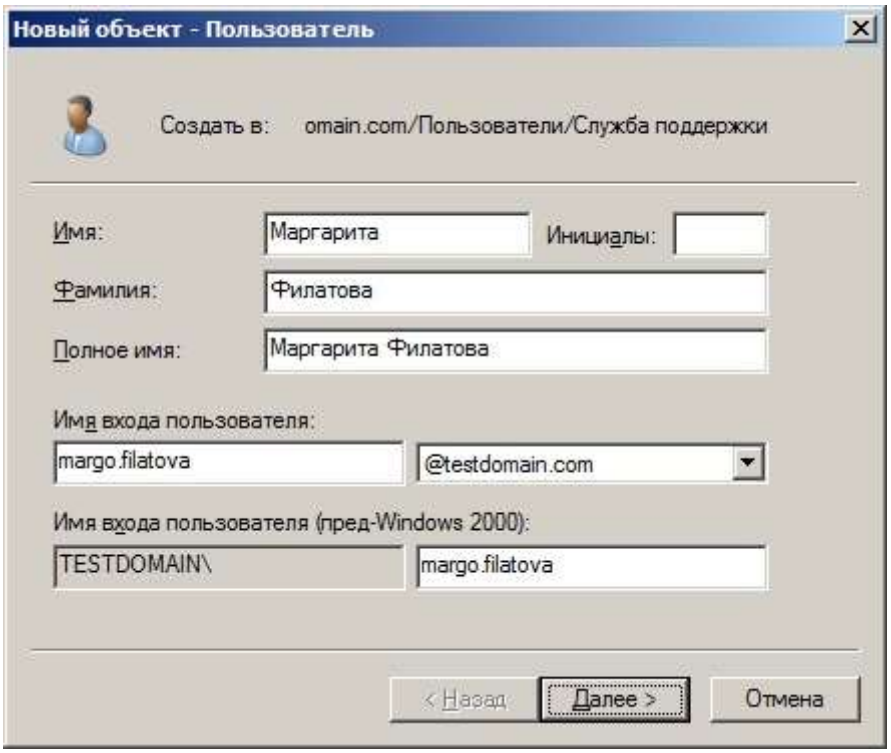


Рис. 2. Диалоговое окно создания пользовательской учетной записи

4. На следующей странице мастера создания пользовательской учетной записи вам предстоит ввести начальный пароль пользователя в поле **«Пароль»** и подтвердить его в поле **«Подтверждение»**. Помимо этого, вы можете выбрать атрибут, указывающий на то, что при первом входе пользователя в систему пользователь должен самостоятельно изменить пароль для своей учетной записи. Лучше всего использовать эту опцию в связке с локальными политиками безопасности **«Политика паролей»**, что позволит создавать надежные пароли для ваших пользователей. Также, установив флажок на опции **«Запретить смену пароля пользователем»** вы предоставляете пользователю свой пароль и запрещаете его изменять. При выборе опции **«Срок действия пароля не ограничен»** у пароля учетной записи пользователя срок действия пароля никогда не истечет и не будет необходимости в его периодическом изменении. Если вы установите флажок **«Отключить учетную запись»**, то данная учетная запись будет не предназначена для дальнейшей работы и пользователь с такой учетной записью не сможет выполнить вход до ее включения. Данная опция, как и большинство атрибутов, будет рассмотрена в следующем разделе данной статьи. После выбора всех атрибутов, нажмите на кнопку **«Далее»**. Эта страница мастера изображена на следующей иллюстрации:

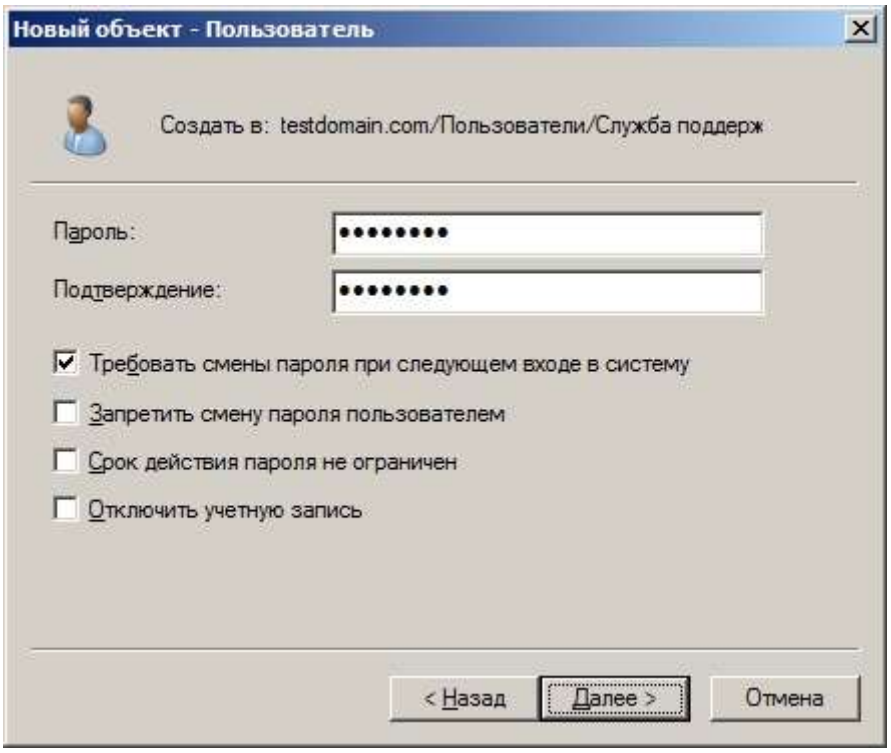


Рис. 3. Создание пароля для создаваемой учетной записи

5. На последней странице мастера вы увидите сводную информацию о введенных вами параметрах. Если информация внесена корректно, нажмите на кнопку **«Готово»** для создания пользовательской учетной записи и завершения работы мастера.
6.

Создание пользователей на основании шаблонов

Обычно в организациях существует множество подразделений или отделов, в которые входят ваши пользователи. В этих подразделениях пользователи обладают схожими свойствами (например, название отдела, должности, номер кабинета и пр.). Для наиболее эффективного управления учетными записями пользователей из одного подразделения, например, используя групповые политики, целесообразно их создавать внутри домена в специальных подразделениях (иначе говоря, контейнерах) на основании шаблонов. **Шаблоном учетной записи** называется учетная запись, впервые появившаяся еще во времена операционных систем Windows NT, в которой заранее заполнены общие для всех создаваемых пользователей атрибуты. Для того чтобы создать шаблон учетной записи пользователя, выполните следующие действия:

1. Откройте оснастку **«Active Directory – пользователи и компьютеры»** и создайте стандартную учетную запись пользователя. При создании такой учетной записи желательно чтобы в списке пользователей в подразделении имя данной записи выделялось из общего списка, и всегда было расположено на видном месте. Например, чтобы такая учетная запись всегда находилось первой, задайте для создаваемого шаблона имя с нижними подчеркиваниями, например, _Маркетинг_. Также, на странице ввода пароля установите флажок **«Отключить учетную запись»**. Так как эта запись будет использоваться только в качестве шаблона, она должна быть отключена;
2. В области сведений оснастки выберите созданную вами учетную запись (значок объекта данной учетной записи будет содержать стрелку, направленную вниз, что означает, что данная учетная запись отключена), нажмите на ней правой кнопкой мыши и из контекстного меню выберите команду **«Свойства»**;

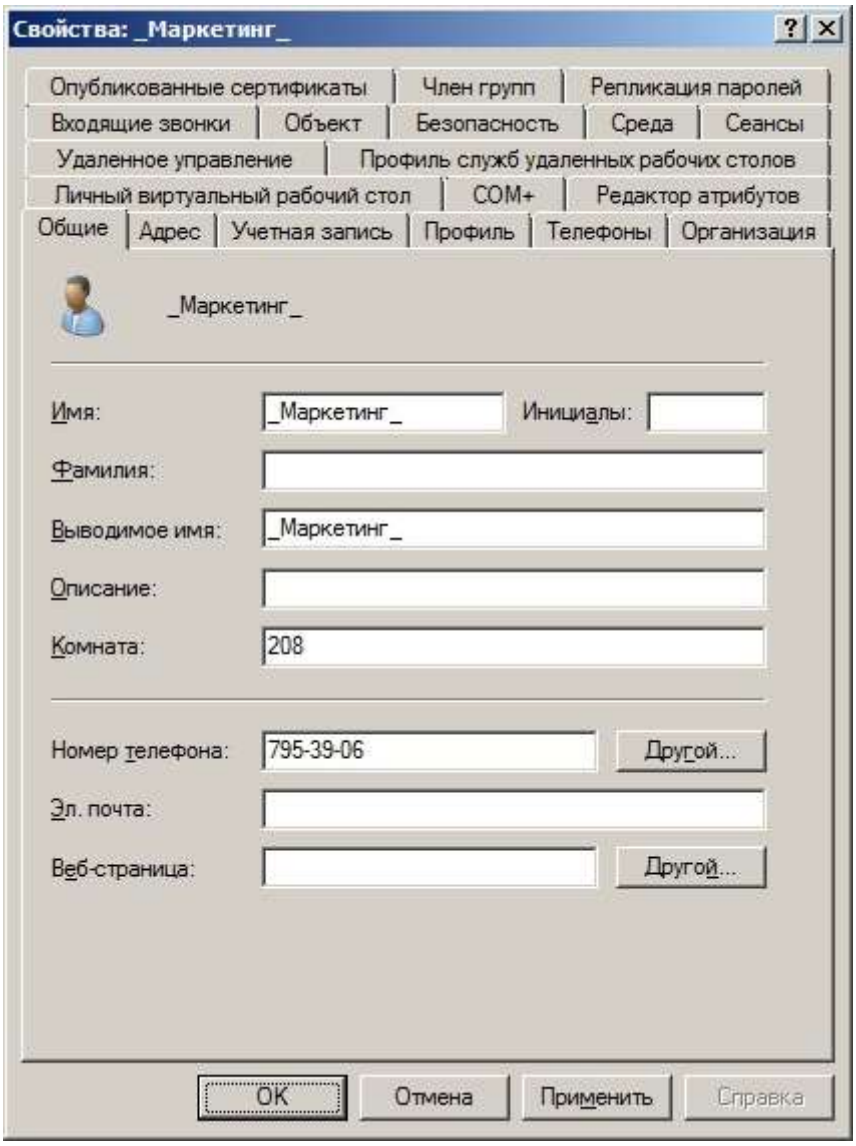


Рис. 4. Свойства учетной записи пользователя

3. Для того чтобы некоторые атрибуты продублировались в свойствах учетных записей пользователей, которые в последствии будут создаваться на основании вашего шаблона, нужно заполнить необходимые для вас поля в свойствах шаблона учетной записи. Вкладки, которые чаще всего используются при редактировании свойств учетных записей, предоставлены ниже:
    - **Общие**. Данная вкладка предназначена для заполнения индивидуальных пользовательских атрибутов. К этим атрибутам относятся имя пользователя и его фамилия, краткое описания для учетной записи, контактный телефон пользователя, номер комнаты, его электронный ящик, а также веб-сайт. Ввиду того, что данная информация является индивидуальной для каждого отдельного пользователя, данные заполненные на этой вкладке не копируются;
    - **Адрес**. На текущей вкладке вы можете заполнить почтовый ящик, город, область, почтовый индекс и страну, где проживают пользователи, которые будут созданы на основании данного шаблона. Так как у каждого пользователя названия улиц обычно не совпадают, данные из этого поля не подлежат копированию;
    - **Учетная запись**. В этой вкладке вы можете указать точно время входа пользователя, компьютеры, на которые смогут заходить пользователи, такие параметры учетных записей как хранение паролей, типы шифрования и пр., а также срок действия учетной записи;
    - **Профиль**. Текущая вкладка позволяет вам указать путь к профилю, сценарий входа, локальный путь к домашней папке, а также сетевые диски, на которых будет размещена домашняя папка учетной записи;
    - **Организация**. На этой вкладке вы можете указать должность сотрудников, отдел, в котором они работают, название организации, а также имя руководителя отдела;
    - **Члены групп**. Здесь указывается основная группа и членство в группах.

    Это основные вкладки, которые заполняются при создании шаблонов учетной записи. Помимо этих шести вкладок, вы можете еще заполнять информацию в 13 вкладках. Большинство из этих вкладок будут рассмотрены в последующих статьях данного цикла.

4. На следующем шагу создается учетная запись пользователя, основанная на текущем шаблоне. Для этого нажмите правой кнопкой мыши на шаблоне учетной записи и из контекстного меню выберите команду **«Копировать»**;
5. В диалоговом окне **«Копировать объект - Пользователь»** введите имя, фамилию, а также имя входа пользователя. На следующей странице введите пароль и подтверждение, а также снимите флажок с опции **«Отключить учетную запись»**. Завершите работу мастера;

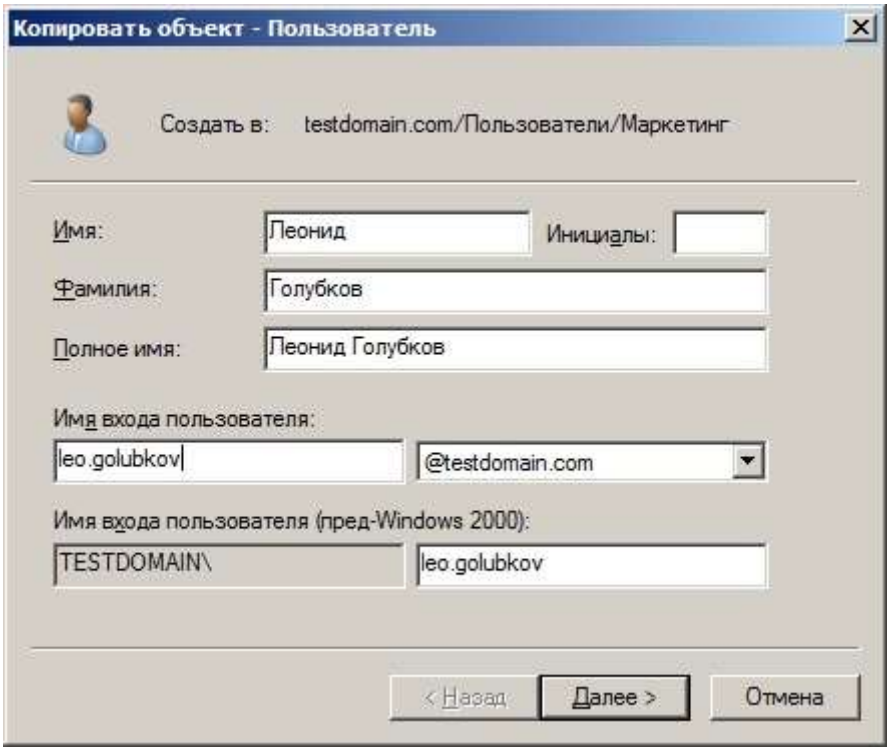


Рис. 5. Диалоговое окно копирования пользовательской учетной записи

6. После создания учетной записи перейдите в свойства созданной учетной записи и просмотрите добавляемые вами свойства в шаблон. Отконфигурированные атрибуты будут скопированы в новую учетную запись.
7.

Создание пользователей средствами командной строки

Как и в большинстве случаев, в операционной системе Windows есть утилиты командной строки с аналогичными функциями графического пользовательского интерфейса оснастки **«Active Directory – пользователи и компьютеры»**. Такие команды называются командами DS, так как они начинаются с букв DS. Для создания принципалов безопасности используется команда **Dsadd**. После самой команды указываются модификаторы, которые определяют тип и имя DN объекта. В случае с созданием учетных записей пользователей вам нужно указать модификатор **user**, который является типом объекта. После типа объекта необходимо ввести DN имя самого объекта. DN (Distinguished Name) объекта является результирующим набором, который содержит отличительное имя. Следом за DN обычно указывают имя пользователя UPN или имя входа предыдущих версий Windows. Если в имени DN присутствуют пробелы, то такое имя нужно заключить в кавычки. Синтаксис команды следующий:

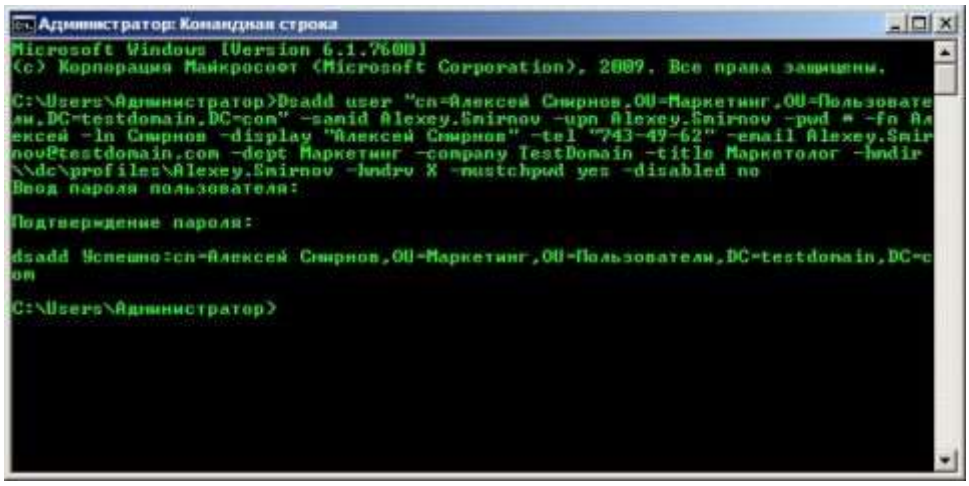
```
Dsadd user DN_имя –samid имя_учетной_записи –UPN_имя –pwd пароль –дополнительные параметры
```

С данной командой можно использовать 41 параметр. Рассмотрим самые распространенные из них:
-samid – имя учетной записи пользователя;
-upn – имя входа пользователя пред-Windows 2000;
-fn – имя пользователя, которое в графическом интерфейсе заполняется в поле **«Имя»**;
-mi – инициал пользователя;
-ln – фамилия пользователя, указываемая в поле «Фамилия» мастера создания пользовательской учетной записи;
-display – указывает полное имя пользователя, которое автоматически генерируется в пользовательском интерфейсе;
-empid – код сотрудника, который создается для пользователя;
-pwd – параметр, определяющий пользовательский пароль. В том случае, если вы укажете символ звездочки (*), вам будет предложено ввести пароль пользователя в защищенном от просмотра режиме;
-desc – краткое описание для пользовательской учетной записи;
-memberof – параметр, определяющий членство пользователя в одной или нескольких группах;
-office – местонахождения офиса, где работает пользователь. В свойствах учетной записи этот параметр можно найти во вкладке **«Организация»**;
-tel – номер контактного телефона текущего пользователя;
-email – адрес электронной почты пользователя, который можно найти во вкладке **«Общие»**;
-hometel – параметр, указывающий номер домашнего телефона пользователя;
-mobile – телефонный номер мобильного пользователя;
-fax – номер факсимильного аппарата, который использует текущий пользователь;
-title – должность пользователя в данной организации;
-dept – этот параметр позволяет указать наименование отдела, в котором работает данный пользователь;
-company – название компании, в которой работает создаваемый пользователь;
-hmdir – основной каталог пользователя, в котором будут расположены его документы;
-hmdrv – путь к сетевому диску, на котором будет размещена домашняя папка учетной записи
-profile – путь профиля пользователя;
-mustchpwd – данный параметр указывает на то, что при последующем входе в систему пользователь обязан изменить свой пароль;
-canchpwd – параметр, определяющий, должен ли пользователь изменять свой пароль. Если значением параметра указано **«yes»**, то у пользователя будет возможность изменения пароля;
-reversiblepwd – текущий параметр определяет хранение пароля пользователя с применением обратного шифрования;
-pwdneverexpires – параметр, указывающий на то, что срок действия пароля никогда не истечет. Во всех этих четырех параметрах, значениями могут выступать только **«yes»** или **«no»**;
-acctexpires – параметр, определяющий, через сколько дней срок действия учетной записи истечет. Положительное значение представляет собой количество дней, через которое учетная запись истечет, а отрицательное означает, что срок действия уже закончен;
-disabled – указывает, что учетная запись уже отключена. Значениями для этого параметра также выступают **«yes»** или **«no»**;
-q – указание тихого режима для обработки команды.
Пример использования:

```
Dsadd user “cn=Алексей Смирнов,OU=Маркетинг,OU=Пользователи,DC=testdomain,DC=com” -samid
Alexey.Smirnov -upn Alexey.Smirnov

-pwd * -fn Алексей -ln Смирнов -display “Алексей Смирнов” -tel “743-49-62” -email
Alexey.Smirnov@testdomain.com -dept Маркетинг

-company TestDomain -title Маркетолог -hmdir \\dc\profiles\Alexey.Smirnov -hmdrv X -mustchpwd yes
-disabled no
```


Администратор: Командная строка
Microsoft Windows [Version 6.1.7600]
(c) Корпорация Майкрософт (Microsoft Corporation), 2009. Все права защищены.
C:\Users\Администратор>Dsadd user "cn=Алексей Смирнов,OU=Маркетинг,OU=Пользовате
ли,DC=testdomain,DC=com" -samid Alexey.Smirnov -upn Alexey.Smirnov -pwd * -fn Ал
ексей -ln Смирнов -display "Алексей Смирнов" -tel "743-49-62" -email Alexey.Smir
nov@testdomain.com -dept Маркетинг -company TestDomain -title Маркетолог -hmdir
\\dc\profiles\Alexey.Smirnov -hmdrv X -mustchpwd yes -disabled no
Ввод пароля пользователя:
Подтверждение пароля:
dsadd Успешно:cn=Алексей Смирнов,OU=Маркетинг,OU=Пользователи,DC=testdomain,DC=c
om
C:\Users\Администратор>