

Управляем объектами в Active Directory

Часть 1

Иван Коробко

Управление объектами в Active Directory осуществляется с помощью соответствующих мастеров. Какие поля при этом изменяются в каталоге Active Directory – покрыто тайной.

Внутренняя структура каталога Active Directory гораздо сложнее, чем кажется на первый взгляд. Всем известно, что управление объектами в Active Directory осуществляется с помощью графической оболочки, встроенного мастера или с помощью сценария. Существует множество литературы, в которой рассказано, как написать сценарий, создающий учетную запись пользователя, прописана пошаговая работа мастера. Однако мне не удалось найти статью, в которой четко была бы описана взаимосвязь полей мастера и полей объекта Active Directory.

Создание каждого сценария для начинающего программиста или системного администратора – это битва. Чтобы ее выиграть, необходимо проявить смекалку и сообразитель-

ность, перерывать множество источников. Не проще ли, как говорят, поставить все точки над «i»?

Типы объектов в Active Directory

Каталог Active Directory поддерживает 8 основных типов объектов (см. **таблицу 1**), каждый из которых описывается набором свойств. Часть из них повторяется, часть – индивидуальна. С другой стороны значения некоторых полей можно просмотреть и изменить с помощью встроенного в Active Directory мастера, а часть – только с помощью специализированного программного обеспечения или сценария.

Тип объекта определяется набором параметров, которые хранятся в Active Directory в массиве objectClass. Некоторые значения присутствуют везде,

например Top, другие строго идентифицируют объект. Избыточность значений необходима для совместимости доменов, построенных на основе Windows 2K и Windows NT.

При составлении поисковых запросов в качестве фильтра используются только индивидуальные значения массива objectClass для однозначной идентификации. Значения многих элементов объектов разных типов пересекаются.

Механизм поиска объектов рассмотрим после того, как вы получите представление об объектной модели Active Directory.

Параметры объектов в Active Directory

Все параметры объектов можно разделить на три группы:

- **Явно задаваемые.** Значения этих параметров напрямую задаются системным администратором. Самый яркий пример – имя объекта.
- **Неявно определяемые.** Эти параметры администратор задает завуалированно. К ним относятся тип и местоположение объекта.
- **Скрытые объекты.** Эти объекты создаются или изменяются системой. С помощью сценария или мастера их, как правило, невозможно изменить. К таким параметрам относятся SID и GUID объекта, время создания объекта.

Объектная модель Active Directory

Не так давно на сайте Microsoft появилось описание полей Active Directory ([http://msdn2.microsoft.com/en-us/library/ms675090\(VS.85\).aspx](http://msdn2.microsoft.com/en-us/library/ms675090(VS.85).aspx)).

Описание сделано в стиле Microsoft, т.е. использовать эту информацию по принципу «как есть» невозможно. В ней приведена вся схема каталога в ужасно сокращенном виде, без примеров.

Чтобы посмотреть «начинку» объекта, рекомендуется использовать утилиту (см. **рис. 1**), недавно созданную сотрудниками Microsoft – Active Directory Explorer 1.01 (<http://technet.microsoft.com/en-us/sysinternals/bb963907.aspx>), однако она не так удобна в использовании, как хотелось бы.

Существует более удачный вариант – утилита Softerra LDAP Browser (<http://www.ldapbrowser.com>), о которой я неоднократно упоминал ранее в своих статьях. Безусловно, эта утилита удобнее, но несколько сложнее в использовании.

Управление объектами в Active Directory

Рассмотрим процессы управления объектами с точки зрения взаимосвязей стандартных инструментов, предлагаемых Microsoft, и объектной модели LDAP.

Из ранее перечисленных объектов чаще всего используются следующие: учетная запись пользователя, группа безопасности и папка.

С объектами в Active Directory можно проделывать следующие манипуляции: создавать, читать, изменять (если возможно), удалять и, наконец, искать.

Таблица 1. Взаимосвязь типов объектов Active Directory и значений параметра objectClass

Комментарий	Тип объекта	Значение objectClass	Фрагмент поискового запроса
Учетная запись компьютера	Computer	Top Person OrganizationalPerson User Computer	objectClass='Computer'
Контакт, используется в почтовых приложениях	Contact	Top Person OrganizationalPerson Contact	objectClass='Contact'
Группа безопасности	Group	Top Group	objectClass='Group'
Учетная запись пользователя, не совместимая с доменами Windows 2k	InetOrgPerson	Top Person OrganizationalPerson User InetOrgPerson	objectClass='InetOrgPerson'
Папка дерева каталогов Active Directory	OU	top organizationalUnit	objectClass='organizationalUnit'
Опубликованный в Active Directory сетевой принтер	Printer	Top Leaf ConnectionPoint PrintQueue	objectClass='PrintQueue'
Опубликованная в Active Directory сетевая папка	Shared Folder	Top Leaf ConnectionPoint Volume	objectClass='Volume'
Учетная запись пользователя, совместимая с доменами Windows NT	User	Top Person OrganizationalPerson User	objectClass='user' and not objectClass='computer'

Рассмотрим подробнее каждое из этих действий на примере работы мастера. Начнем с учетной записи пользователя.

Учетная запись пользователя

Рассмотрим процесс создания учетной записи пользователя с помощью мастера и программным способом. Составление этих двух методов позво-

лит читателю понять взаимосвязь полей Active в каталоге Directory и полей в мастере. Сначала рассмотрим основные принципы создания учетной записи.

Создание учетной записи пользователя. Основные принципы

Для инициализации процесса создания учетной записи необходимо запус-

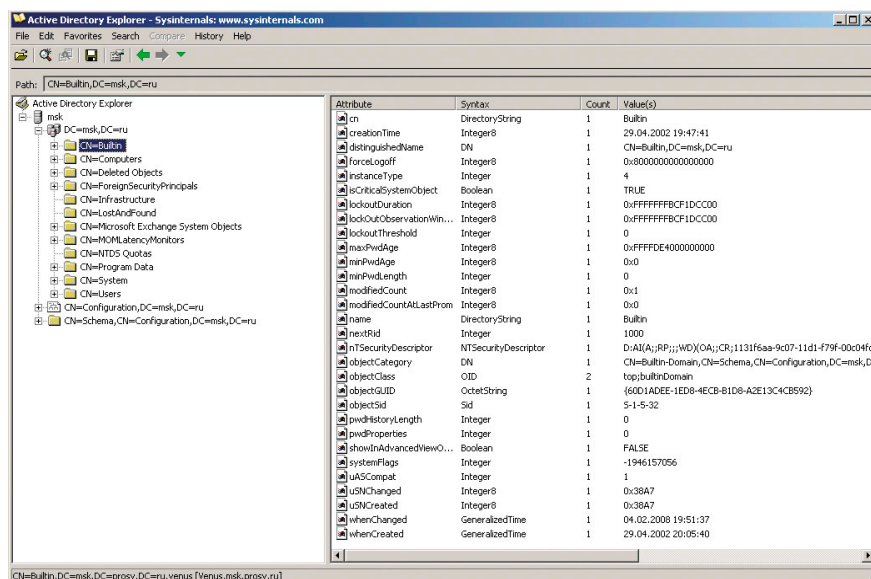


Рисунок 1. Внешний вид программы Active Directory Explorer 1.01

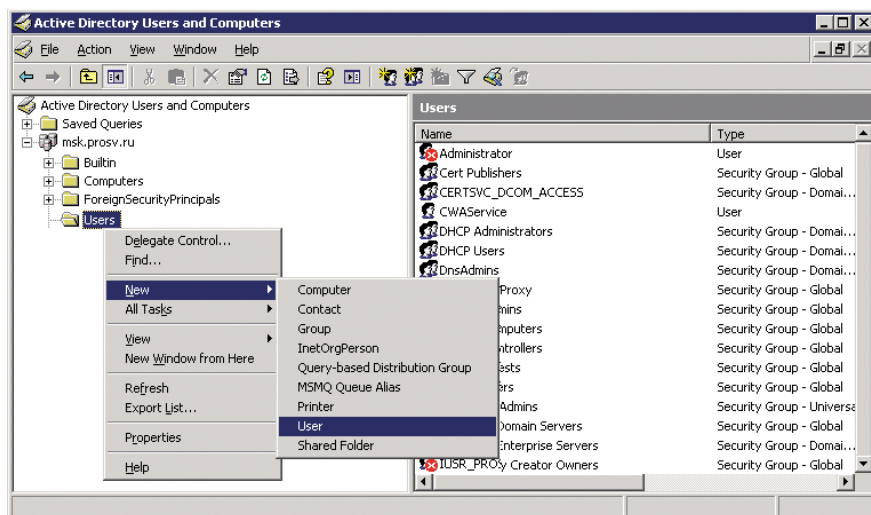


Рисунок 2. Создание учетной записи пользователя

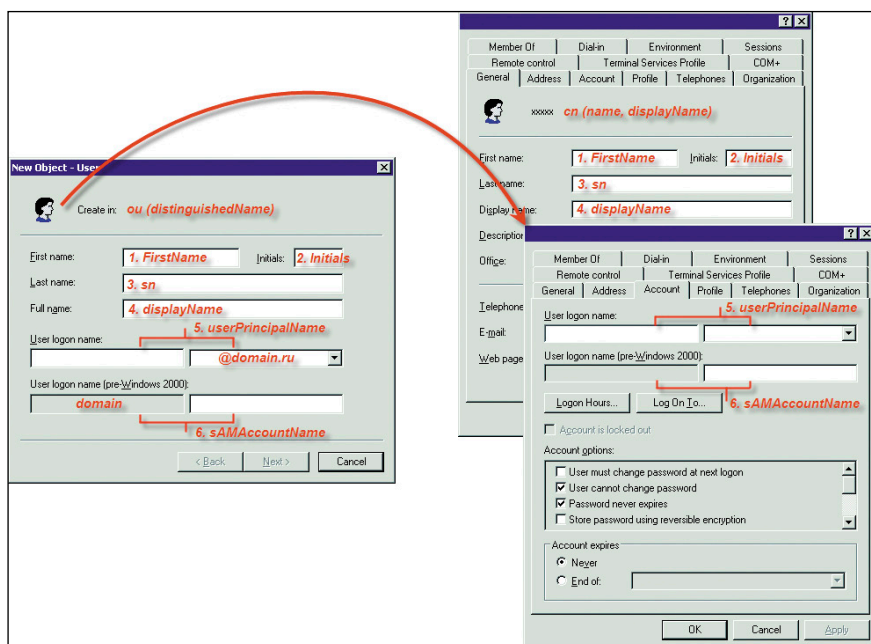


Рисунок 3. Работа мастера «Создание учетной записи пользователя». Шаг 1

твить соответствующий мастер в MMC-оснастке Active Directory. Для этого установите курсор на папку, в которой будет создана учетная запись, и, вызвав контекстное меню папки, выберите в нем пункт «New → User» (см. рис. 2). Выполнив эти действия, системный администратор неявным образом определил местоположение учетной записи будущего пользователя, а именно часть параметра distinguishedName: CN=User,DC=msk, DC=ru и тип объекта – параметра objectClass.

Замечание: если папка является встроенной, то ее имя определяется параметром CN. Все остальные параметры идентифицируются параметром OU (Organizational Unit), например OU=Test,CN=User,DC=msk, DC=ru.

Работа мастера состоит из трех частей. Рассмотрим последовательно каждую из них.

Во время создания учетной записи пользователя на первом шаге необхо-

димо указать фамилию, имя и отчество пользователя. Необязательно задавать все три параметра: достаточно задать один из них. Полное имя (поле 4) формируется на основе Ф.И.О., заданных с помощью первых трех полей. Его значение формируется автоматически, однако администратор может изменить его на любое другое. Первые четыре параметра могут быть позже изменены (см. рис. 3). Для этого необходимо войти в свойства пользователя во вкладку «General» (отображается по умолчанию).

Вторая группа параметров – имя пользователя в сети и дополнительное имя, требуемое для связи доменов, построенных на основе Windows NT и Windows 2K. В Active Directory им соответствуют параметры userPrincipal Name и sAMAccountname. Каждое из этих имен состоит из двух частей: имени пользователя и текущего домена. Имя текущего домена определяется автоматически и не может быть изменено. В таблице 2 приведено описание полей, задействованных на первом шаге работы мастера.

На втором этапе работы мастера администратор задает пароль пользователя, длина которого определяется доменной политикой безопасности «Minimum Password Length», расположенной в «Computer Configuration → Windows Settings → Security Settings → Account Policies → Password Policy» оснастки групповых политик. Определяется политика безопасности учетной записи.

На рис. 4 показано, какими параметрами Active Directory может управлять системный администратор на этапе создания учетной записи пользователя.

К этим параметрам относятся:

Таблица 2. Параметры учетной записи пользователя. Шаг 1

Параметр мастера	Поле в Active Directory	Тип данных	Вкладка в свойствах объекта USER	Описание
First name	firstName	String	General	Имя сотрудника
Initials	Initials	String	General	Инициалы (до 6 символов)
Last name	Sn	String	General	Фамилия сотрудника
Full name	displayName	String	General	Полное имя сотрудника (формируется на основе первых трех полей)
User logon name	userPrincipalName	String	Account	Имя регистрации пользователя в сети
User logon name (pre-Windows 2000)	sAMAccountname	String	Account	Имя регистрации пользователя в сети для учетных записей Windows NT

- **setPassword**. Значение этого обязательного параметра – пароль, хранящийся в зашифрованном виде в Active Directory. С помощью сценария его можно только записать. Считать существующее не представляется возможным: оно зашифровано.
- **pwdLastSet**. Значением параметра pwdLastSet управляют с помощью «User must change password at next logon» (см. **рис. 4**). По умолчанию принимает значение 0.
- **userAccountControl**. Оставшиеся три параметра («User cannot change password», «Password never expires» и «Account is disabled») формируют в сумме значение параметра userAccountControl. По умолчанию userAccountControl=513 (стандартная учетная запись пользователя).

Все перечисленные параметры, кроме setPassword, можно изменить во вкладке «Account» учетной записи пользователя.

После завершения второго шага работы мастера перейдем к третьему – завершающему этапу, на котором осуществляется проверка ранее заданных параметров (см. **рис. 5**). В диалоговом окне приводится следующая информация:

- местоположение пользователя в Active Directory;
- отображаемое имя пользователя в сети;
- имя пользователя для регистрации в сети;
- параметры безопасности, которые устанавливаются на втором шаге работы мастера.

На этом этапе невозможно напрямую изменить какие-либо данные. Для корректировки параметров необходимо вернуться на шаг или два шага назад (см. **рис. 5**).

Создание учетной записи пользователя. Работа мастера

Создадим учетную запись пользователя с помощью мастера. Исходные данные приведены в **таблице 3**.

Рассмотрим пошагово создание учетной записи.

В появившемся диалоговом окне заполните поля в соответствии с данными, приведенными в колонке «Зна-

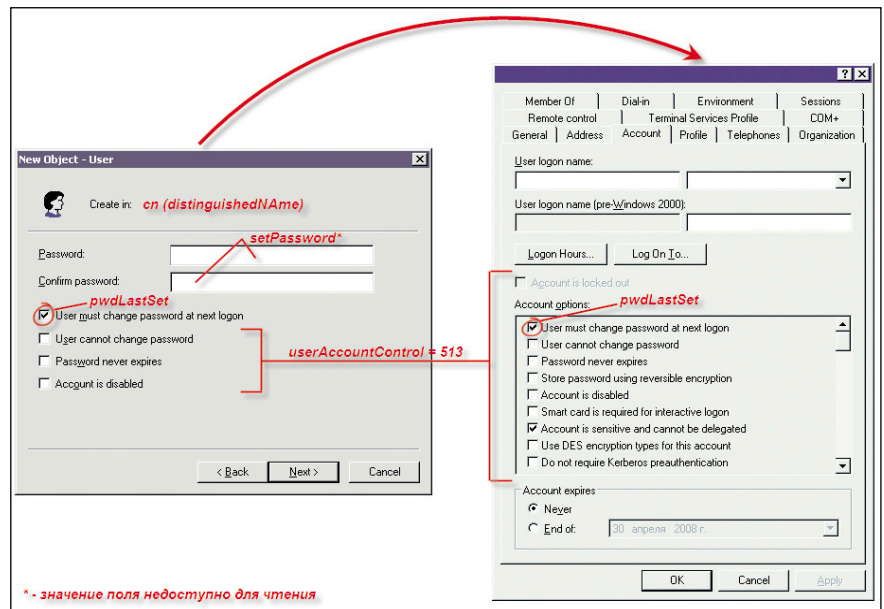


Рисунок 4. Работа мастера «Создание учетной записи пользователя». Шаг 2

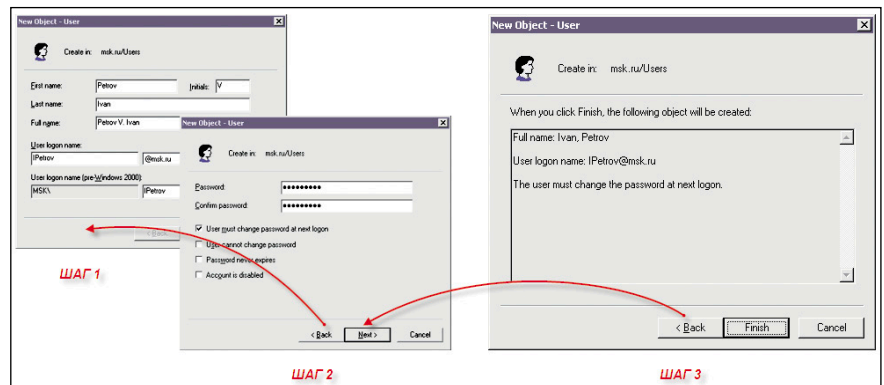


Рисунок 5. Работа мастера «Создание учетной записи пользователя». Шаг 3

Таблица 3. Исходные данные для создания учетной записи пользователя

Поля мастера	Значение	Комментарий
Create In	MSK\Users	Встроенная в корневой каталог домена папка Users
Шаг 1		
First name	Petrov	Фамилия
Initials	V	Инициал
Last name	Ivan	Отчество
Full name	Petrov, Ivan	Отображаемое имя
User logon name	IPetrov	Имя для входа в сеть
User logon name (pre-Windows 2000)	Petrov	Имя для входа в сеть (для совместимости с Windows NT доменами)
Шаг 2		
Password, Confirm password	123456789	Пароль
User must change password at next logon	Да	Пользователь должен изменить пароль после первого входа в сеть
User cannot change password	Нет	Пользователь не может изменить пароль
Password never expires	Нет	Действие пароля неограниченно
Account is disabled	Нет	Учетная запись выключена

чение» **таблицы 3**. Обратите внимание, что после заполнения первых трех полей при переходе на четвертое оно заполняется автоматически (см. **рис. 6**).

Имя пользователя для регистрации в сети задается системным администратором. На основе введенных данных автоматически создается имя для под-

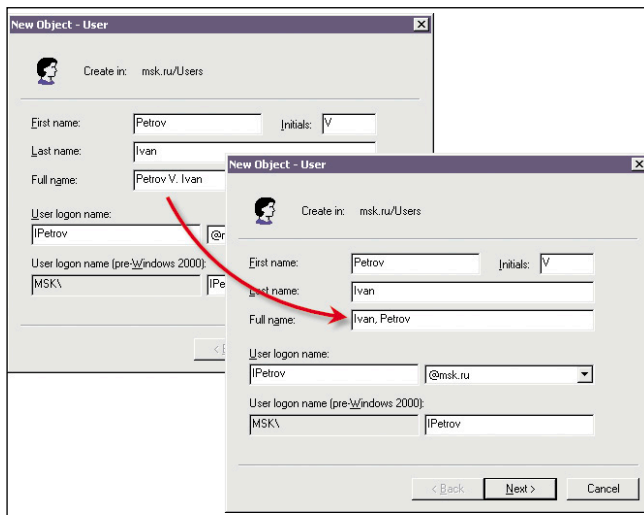


Рисунок 6. Работа мастера. Шаг 1

держки доверительных отношений с доменом Windows NT, которое может быть изменено.

На втором шаге необходимо ввести пароль и подтвердить его. По назначению пароля существуют следующие рекомендации:

- пароли чувствительны к регистру символов;
- используйте цифры в паролях;
- рекомендуемая длина пароля – не менее 7 символов;
- в пароле не использовать символы «\|:;,+*?<>;
- не используйте в пароле имя учетной записи пользователя;
- не используйте очевидных паролей, вроде 0123456789.

Контроль за выполнением некоторых из перечисленных требований может быть возложен на доменные групповые политики. Остальные четыре параметра безопасности оставим без изменений (см. рис. 7).

На последнем, завершающем этапе, осуществляется контроль установленных параметров (см. рис. 8).

Программное создание учетной записи пользователя

Во время создания учетной записи пользователя программным способом (VBScript), как при работе мастера, должны быть обязательно заданы несколько параметров. В листинге 1 приведен сценарий, позволяющий создать учетную запись пользователя. Результат действия сценария идентичен работе мастера, который был рассмотрен в преды-

дущем разделе. В таблице 4 приведены параметры и соответствующие им значения, которые необходимо задать в Active Directory.

Сценарий работает по следующему алгоритму: сначала определяется имя текущего домена с помощью обращения к виртуальному объекту RootDSE и трансформируется с помощью функции DetectDNSName в короткое имя домена. В сценарии используется составное и сокращенное имя домена. Составное имя домена участвует в формировании пути к создаваемому объекту, сокращенное – для назначения имени объекта, совместимого с доменами Windows NT.

Далее создается объект с помощью функции Create. В качестве ее параметров задается имя объекта и его тип. Задаются значения параметров с помощью функции Put и их запись в каталог Active Directory с помощью метода SetInfo.

Листинг 1. Создание учетной записи пользователя

```
set RootDSE = GetObject("LDAP://RootDSE")
Domain = rootDSE.Get("defaultNamingContext")
Set objUsers = GetObject("LDAP://CN=Users," & Domain)
Set objNewUser = objUsers.Create("user", "cn=Ivan\, Petrov")

objNewUser.Put "sAMAccountName", "IPetrov"
objNewUser.Put "sn", "Petrov"
objNewUser.Put "givenName", "Ivan"
objNewUser.Put "Initials", "V"
objNewUser.Put "userPrincipalName", "IPetrov@" & _
    DetectDNSName(Domain)
objNewUser.SetInfo
objNewUser.AccountDisabled=False
objNewUser.SetPassword("1234567890")
objNewUser.SetInfo

Function DetectDNSName(Domain)
' Определение DNS-имени домена
LDAPArray = Split(Domain, ",")
For Each el In LDAPArray
    DNSName = DNSName + right(el,Len(el)-3) + "."
Next
DetectDNSName = left(DNSName, Len(DNSName)-1)
End Function
```

В приведенном сценарии есть несколько особенностей, на которые необходимо обратить внимание:

- Для того чтобы в имени учетной записи (поле CN) присутствовала запятая, необходимо при присвоении значения перед запятой поставить косую черту (\): «cn=Ivan\, Petrov». В противном случае интерпретатор VBScript выдаст сообщение об ошибке (см. рис. 10).
- Значение параметра userPrincipalName содержит суффикс, в данном случае @msk.ru. Им является DNS-имя текущего домена. В сценарии присутствует функция DetectDNSName, которая преобразует LDAP-имя в DNS-имя.

- Значение свойства AccountDisabled не может быть изменено, пока объект не существует, поэтому метод SetInfo в скрипте используется дважды.

В результате работы мастера или рассмотренного сценария в Active Directory создается учетная запись пользователя. Уверен, что все администраторы сети видели ее в стандартной оснастке Active Directory, однако мало кто видел, как на самом деле вы-

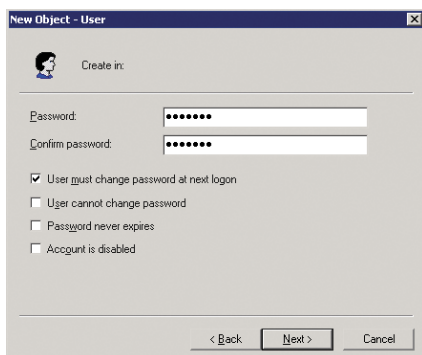


Рисунок 7. Работа мастера. Шаг 2

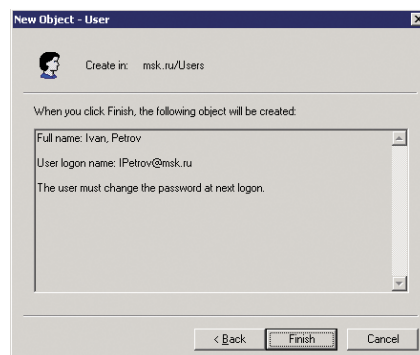


Рисунок 8. Работа мастера. Шаг 3

глядит самая обыкновенная учетная запись пользователя, созданная обычным мастером. На **рис. 9** представлены все поля созданной учетной записи. Как видно, одни атрибуты были заданы напрямую, другие – косвенным образом, третьи были созданы системой автоматически. О том, какие бывают атрибуты, как считывать их значения, речь пойдет в следующей статье.

Создание объектов. Общий случай

После подробного рассмотрения процесса создания учетной записи пользователя, пришло время подвести своеобразный итог и создать шаблон (см. **листинг 2**), позволяющий создавать учетные записи объектов различного типа. Для создания какого-либо объекта необходимо задать минимум три параметра и еще несколько параметров, присущих объекту данного типа. К обязательным параметрам относят путь к объекту, его имя и тип.

Name	Value	Type	Size
accountExpires	9223372036854775807	text attribute	19
badPasswordTime	0	text attribute	1
badPwdCount	0	text attribute	1
cn	Ivan, Petrov	text attribute	12
codePage	0	text attribute	1
countryCode	0	text attribute	1
createTimeStamp	20080410090637.0Z	operational attribute	17
displayName	Ivan, Petrov	text attribute	12
distinguishedName	CN=Ivan\, Petrov,CN=Users,DC=msk,DC=ru	text attribute	47
givenName	Petrov	text attribute	6
initials	V	text attribute	1
instanceType	4	text attribute	1
lastLogoff	0	text attribute	1
lastLogon	0	text attribute	1
logonCount	0	text attribute	1
modifyTimeStamp	20080410090637.0Z	operational attribute	17
name	Ivan, Petrov	text attribute	12
objectCategory	CN=Person,CN=Schema,CN=Configuration,DC=msk,DC=ru	text attribute	58
objectClass	top	text attribute	3
objectClass	person	text attribute	6
objectClass	organizationalPerson	text attribute	20
objectClass	user	text attribute	4
objectGUID	F7 C5 CC CD 1B 4D A4 44 B4 24 72 43 4C 85 C0 98	binary attribute	16
objectSid	01 05 00 00 00 00 05 15 00 00 00 2C 8F EC FB	binary attribute	28
primaryGroupID	513	text attribute	3
pwdLastSet	0	text attribute	1
sAMAccountName	IPetrov	text attribute	7
sAMAccountType	805306368	text attribute	9
sn	Ivan	text attribute	4
subSchemaSubEntry	CN=Aggregate,CN=Schema,CN=Configuration,DC=msk,DC=ru	operational attribute	61
userAccountControl	512	text attribute	3
userPrincipalName	IPetrov@msk.ru	text attribute	20
uSNChanged	794175	text attribute	6
uSNCreated	794169	text attribute	6
whenChanged	20080410090637.0Z	text attribute	17
whenCreated	20080410090637.0Z	text attribute	17

Рисунок 9. Параметры учетной записи пользователя, созданной с помощью мастера

Листинг 2. Шаблон создания объектов в Active Directory

```
set RootDSE = GetObject("LDAP://RootDSE")
Domain = rootDSE.Get("defaultNamingContext")
Set objs = GetObject("LDAP://" + ПУТЬ К ПАПКЕ + " & Domain)
Set obj = objs.Create("ТИП ОБЪЕКТА", "ИМЯ ОБЪЕКТА")

obj.Put "ПОЛЕ ТИПА СТРОКА В ACTIVE DIRECTORY", "ЗНАЧЕНИЕ"
obj.Put "ПОЛЕ ТИПА МАССИВ В ACTIVE DIRECTORY", Array("ЗНАЧЕНИЕ1", "ЗНАЧЕНИЕ2", "ЗНАЧЕНИЕ3"... )

obj.SetInfo
```

В первых двух строках шаблона с помощью виртуального объекта RootDSE определяют LDAP-имя текущего домена.

Таблица 4. Параметры сценария для создания учетной записи пользователя

Параметр	Комментарий
cn=Ivan\, Petrov	Отображаемое имя
sAMAccountName = IPetrov	Имя в сети для совместимости с доменами Windows NT
Sn = Petrov	Фамилия
givenName = Ivan	Имя
Initials = V	Инициалы
userPrincipalName = IPetrov@msk.ru	Имя в сети домена Windows 2K
SetPassword=123456789	Назначаемый пароль
pwdLastSet=0	Изменить пароль при следующем входе в сеть
distinguishedName = CN=Ivan\, Petrov,CN=Users,DC=msk,DC=ru	Путь к создаваемой учетной записи

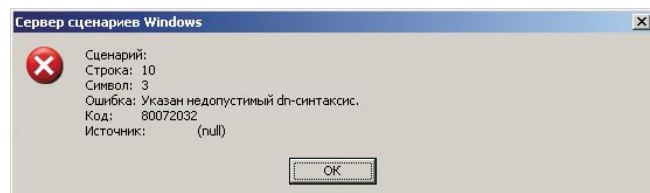


Рисунок 10. VBScript. Ошибка работы сценария

на. С помощью функции GetObject() получают доступ к папке, в которой будет создан объект. На четвертой строке с помощью функции Create(), имеющей два параметра, создается объект. Первый параметр функции – тип создаваемого объекта, второй – его имя в домене. Далее, с помощью функции Put(), осуществляется присваивание значений характерным параметрам. И, наконец, запись присвоенных данных в каталог с помощью функции SetInfo().

Обратите внимание на последние две строки шаблона. В них осуществляется присваивание значений параметру, который имеет строковый тип данных, и массиву из строк. При задании значений массиву обязательно используется ключевое слово Array, с помощью которого объявляют и сразу же определяют значения элементов массива. На основе созданного шаблона приведу примеры создания учетной записи группы (см. **листинг 3**) и папки (см. **листинг 4**).

Листинг 3. Создание учетной записи группы безопасности

```
set RootDSE = GetObject("LDAP://RootDSE")
Domain = rootDSE.Get("defaultNamingContext")
Set objGroups = GetObject("LDAP://" & CN=Test,CN=Groups," & \ Domain)
Set objGrou = objGroups.Create("group", "cn=Print Manage")

objGroup.Put "sAMAccountName", "Print Manage"
objGroup.SetInfo
```

Листинг 4. Создание учетной записи папки

```
set RootDSE = GetObject("LDAP://RootDSE")
Domain = rootDSE.Get("defaultNamingContext")
Set objOUs = GetObject("LDAP://" & CN=Users," & Domain)
Set objOU = objOUs.Create("organizationalUnit", "ou=Test")
objOU.SetInfo
```

В следующий раз будет подробно рассмотрена методика чтения различных параметров учетной записи пользователя, различных типов данных.