

Создаём каталог Active Directory

Иван Коробко

Создание каталога Active Directory – ответственное дело. Рассказ об автоматизации этого процесса читайте в статье.

Основной функцией мастера Active Directory Installation Wizard является конфигурирование сервера для его функционирования как контроллера домена в зависимости от текущего состояния Active Directory.

При повышении статуса сервера до уровня контроллера домена новый каталог Active Directory создается в том случае, если домена еще нет. Данный компьютер будет содержать первый домен первого дерева первого леса.

Подготовка к установке Active Directory

Для успешной установки Active Directory в операционной системе Windows должны быть соблюдены следующие условия:

- **Операционная система должна принадлежать к семейству серверов**, т.е. Windows 2000 Server, Windows 2003 Server или Windows 2008 Server.
- **Файловая система, на которую устанавливается Active Directory – NTFS**. Это обусловлено тем, что система безопасности в FAT32 отсутствует. Если файловая система, установленная на сервер – FAT32, то необходимо воспользоваться утилитой convert.exe, входящей в комплект поставки операционной системы, для ее преобразования в NTFS.
- **Сервер должен иметь доступ к DNS-серверу**. Если это условие не выполнено, то мастер установки Active Directory установит службу DNS на сервере и поместит DNS-базу в Active Directory. Другие варианты установки Active Directory будут недоступны. Рекомендуется хранить DNS-базу в отдельном файле. Для соблюдения этого условия необходимо заранее выполнить установку и настройку DNS.
- **На сервере должны быть установлены драйверы для сетевого адаптера и выполнена настройка протокола TCP/IP**. Для сервера рекомендуется назначить статический IP-адрес. Если DNS-сервер присутствует в сети, его адрес также необходимо зафиксировать в свойствах протокола TCP/IP.

Запуск мастера установки Active Directory

Рассмотрим процесс установки каталога Active Directory на Windows Server 2008. Как и в предыдущих версиях Windows, запуск мастера осуществляется запуском утилиты dcpromo.exe. Мастер может работать в трех режимах:

- **Стандартный**. Работа мастера состоит из нескольких шагов. На каждом из них администратор задает исходные данные, касающиеся конфигурации домена. Затем на основе представленной информации осуществляется установка и настройка Active Directory.
- **Расширенный**. Дополняет некоторыми сервисными функциями, которые не будут рассмотрены в этой статье.

Описание параметров файла ответов для создания Active Directory

Параметр	Описание
InstallDNS	Установка службы DNS на сервере. Принимает значение «Yes» или «No». Значение зависит от состояния домена. По умолчанию, при создании нового леса, присваивается значение «Yes»
NewDomain	Указывает тип создаваемого домена: Tree – новый домен является корнем в существующем лесу; Child – новый домен является дочерним по отношению к существующему; Forest (значение по умолчанию) – новый домен является первым в новом лесу деревьев домена
NewDomainDNSName	Новое имя DNS-сервера в формате Fully Qualified Domain Name (FQDN). Пример: Island.RU. По умолчанию не определен
DomainNetBiosName	Сокращенное имя домена. Как правило, ему соответствует первая часть FQDN-имени. Пример: Island. По умолчанию не определен
SiteName	Имя сайта, начинаемое в новом лесу. По умолчанию Default-First-Site-Name. Изменять этот параметр следует только в том случае, если созданных сайтов несколько, поскольку назначенное им будет возвращаться при попытке обратиться к сайту
ReplicaOrNewDomain	Параметр используется только для создания нового домена: Replica – сервер становится дополнительным контроллером домена; ReadOnlyReplica – сервер конвертируется в RODC, характерно только для Windows 2008; Domain – сервер преобразуется в первый контроллер домена
ForestLevel	Число, определяющее функциональный уровень леса в новом домене: 0 = Windows 2000 Server; 2 = Windows Server 2003; 3 = Windows Server 2008. По умолчанию принимает значение 0
DomainLevel	Число, определяющее функциональный уровень домена: 0 = Windows 2000 Server; 2 = Windows Server 2003; 3 = Windows Server 2008. Назначаемое значение основывается на функциональном уровне леса в новом домене. По умолчанию значение не определено
DatabasePath	Полный FQDN-путь (не UNC-путь) к папке на жестком диске локального компьютера, в котором создана база AD DS (файл NTDS.DIT). Если папка существует, то она должна быть пуста. Если папка отсутствует – она будет создана. Для успешного создания базы данных необходимо минимум 200 Мб свободного места на жестком диске. Значение по умолчанию «%systemroot%\NTDS», где NTDS – имя файла базы данных без расширения
LogPath	Полный FQDN-путь (не UNC-путь) к папке на жестком диске локального компьютера, в котором создан журнал событий базы данных AD DS. Значение по умолчанию «%systemroot%\NTDS»
RebootOnCompletion	Перезагрузка сервера после завершения работы мастера. Принимает значение «Yes» (по умолчанию) или «No»
SYSVOLPath	Полный FQDN-путь (не UNC-путь) к папке SYSVOL на жестком диске локального компьютера. Значение по умолчанию «%systemroot%\SYSVOL»
SafeModeAdminPassword	Пароль для входа в Directory Service Restore Mode в случае нарушения работы контроллера домена. Задаваемые значения <PASSWORD> или NONE. По умолчанию не определен

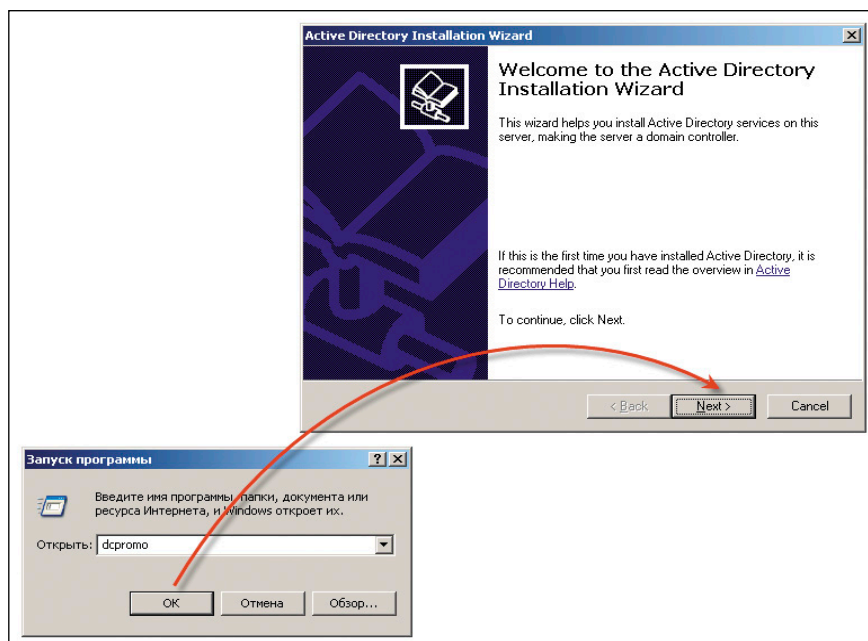


Рисунок 1. Запуск утилиты dcpromo.exe

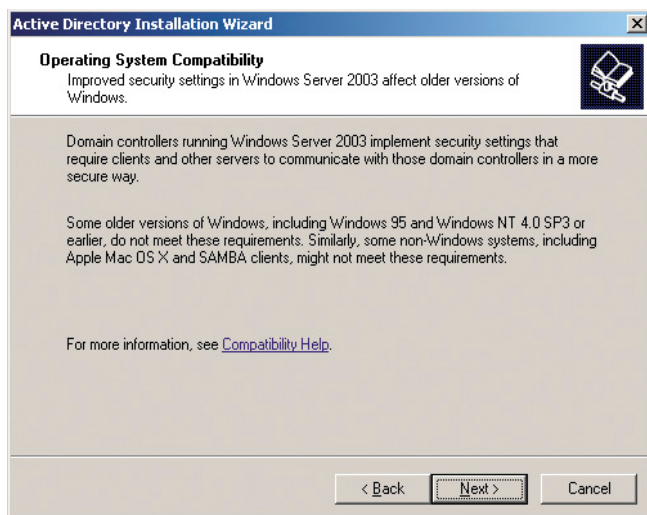


Рисунок 2. Совместимость операционных систем

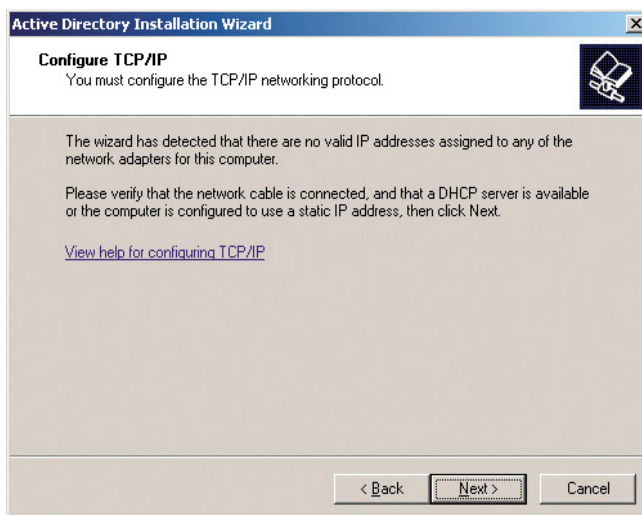


Рисунок 3. Настройка протокола TCP/IP

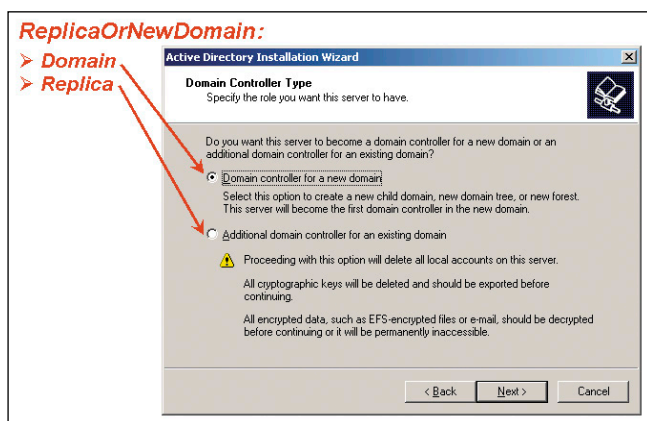


Рисунок 4. Выбор типа контроллера домена

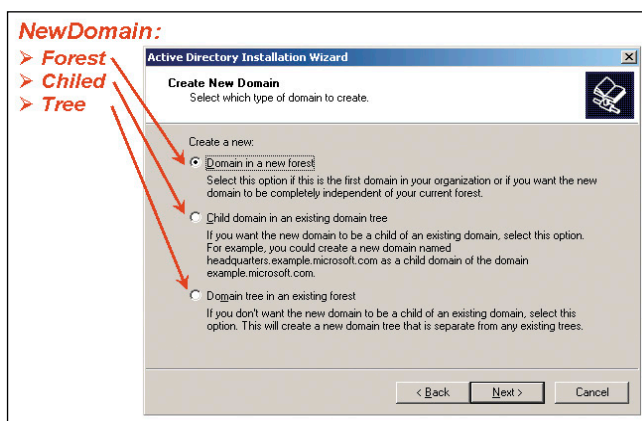


Рисунок 5. Определение типа домена

- **Автоматический с помощью файла ответов.** Все ответы на задаваемые мастером вопросы в обычном/расширенном режиме хранятся в файле ответов. Использование файла ответов экономит системному администратору время и снижает влияние человеческого фактора.

О работе мастера в расширенном и обычном режиме можно прочитать в любом справочнике системного администратора. Остановимся подробнее на установке Active Directory в автоматическом режиме. Утилита dcpromo.exe имеет следующий синтаксис:

- **/unattend:<path to file>** – запуск мастера с файлом ответов;
- **/adv** – включение расширенного режима работы мастера;
- **/?** – вывод справки.

Синтаксис файла ответов утилиты DCPROMO.EXE

Для автоматизации работы мастера рекомендуется создать файл ответов (answer file), который представляет собой текстовый файл в кодировке ASCII. В нем содержатся значения параметров, которые подставляются мастеру во время его работы (см. **ЛИСТИНГ 1**).

[DCINSTALL]

```
InstallDNS = Yes
NewDomain = Forest
NewDomainDNSName = <DNS-имя создаваемого домена>
DomainNetBiosName = <Сокращенное имя домена>
SiteName = <Имя сайта>
ReplicaOrNewDomain = domain
ForestLevel = <Функциональный уровень леса>
DomainLevel = <Функциональный уровень домена>
DatabasePath = <Локальный путь к базе данных>
LogPath = <Локальный путь к файлу отчетов>
RebootOnCompletion = Yes
SYSVOLPath = <Локальный путь к папке System Volume>
SafeModeAdminPassword = <Пароль для входа учетной записи административными правами в случае сбоя работы домена>
```

В шаблоне фигурирует ряд параметров, описание которых приведено в **таблице**.

Пример файла ответов ANSWER.TXT для создания корня домена ISLAND.RU на Windows 2008 Server приведен в **ЛИСТИНГЕ 2**.

```
[DCINSTALL]
InstallDNS = YES
NewDomain = FOREST
NewDomainDNSName = ISLAND.RU
DomainNetBiosName = ISLAND
SiteName = Default-First-Site-Name
ReplicaOrNewDomain = DOMAIN
ForestLevel = 3
DomainLevel = 3
DatabasePath = %systemroot%\NTDS
LogPath = %systemroot%\NTDS
RebootOnCompletion = YES
SYSVOLPath = %systemroot%\SYSVOL
SafeModeAdminPassword = NONE
```


Понимание процесса установки Active Directory

Рассмотрим параллельно работу мастера в стандартном и автоматическом режимах, основываясь на информации, приведенной в файле ответов ISLAND.TXT в листинге 2.

На первом шаге запускается мастер вызовом утилиты dcpromo.exe (см. рис. 1) из меню «Пуск → Выполнить». Для запуска мастера в автоматическом режиме с помощью файла C:\island.txt используйте команду:

```
Dcpromo.exe /unattend:C:\island.txt
```

На втором шаге выводится информация, касающаяся совместимости с точки зрения систем безопасности Windows 2003 Server с другими операционными системами (см. рис. 2).

На третьем шаге осуществляется проверка настройки, конфигурации сетевой карты и протокола TCP/IP. Если система проверки обнаружит какие-либо ошибки, то будет выведено информационное окно (см. рис. 3).

На четвертом шаге (см. рис. 4) определяют тип создаваемого контроллера домена:

- **Domain Controller for a new domain** – установить контроллер домена в новом домене. В файле ответа за выбор этого параметра отвечает параметр ReplicaOrNewDomain = Domain.
- **Additional domain controller for an existing domain** – установить дополнительный контроллер домена в существующем домене. В файле ответа за выбор этого параметра отвечает параметр ReplicaOrNewDomain = Replica.

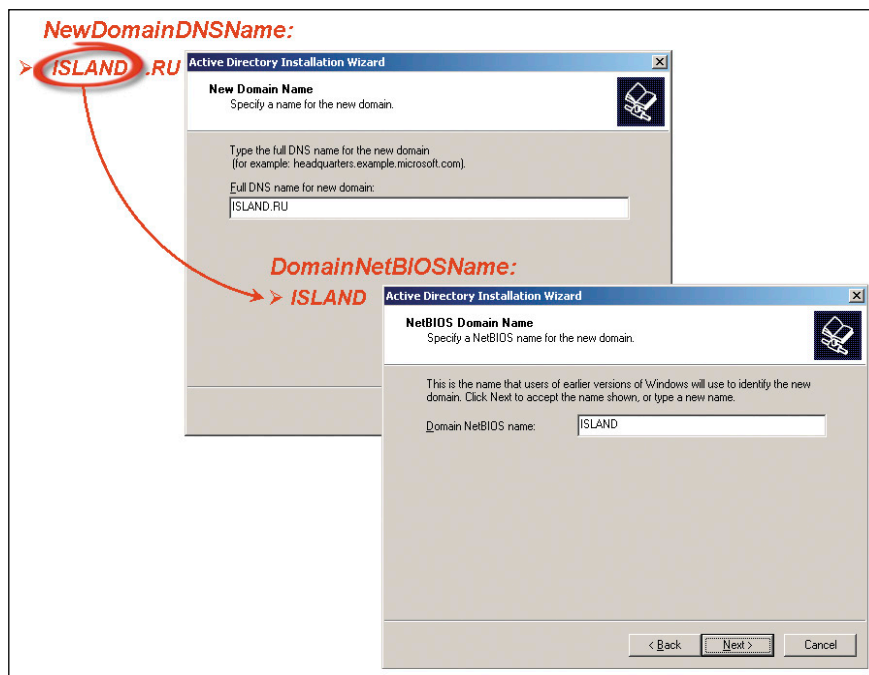


Рисунок 6. Определение DNS- и NetBIOS-имен домена

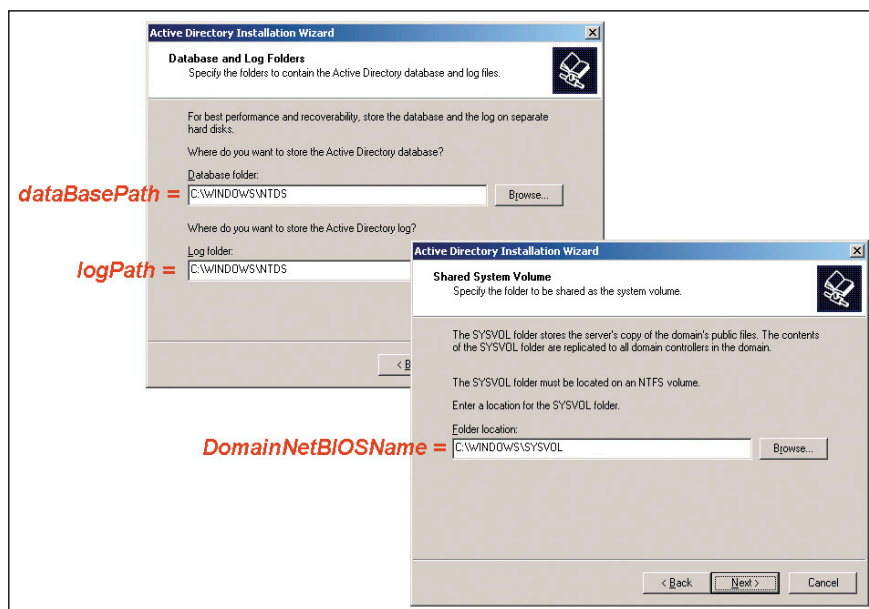


Рисунок 7. Определение физического местоположения базы

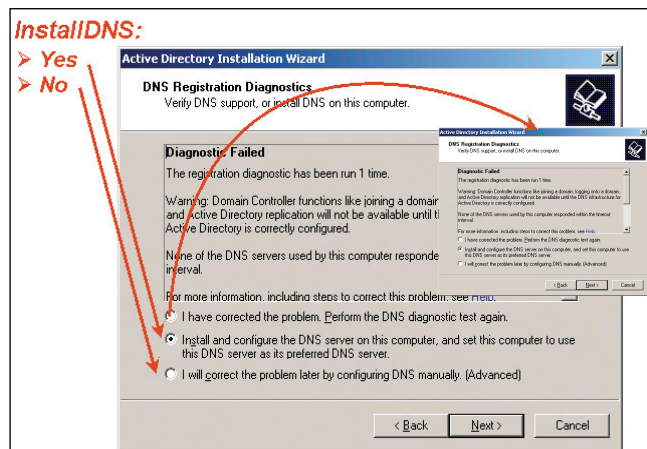


Рисунок 8. Настройка службы DNS

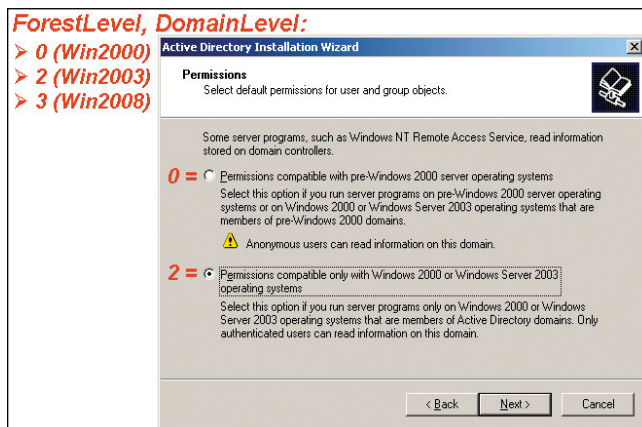


Рисунок 9. Настройка совместимости создаваемого домена с доменами на основе Windows NT



Рисунок 10. Назначение пароля, необходимого для запуска режима восстановления домена

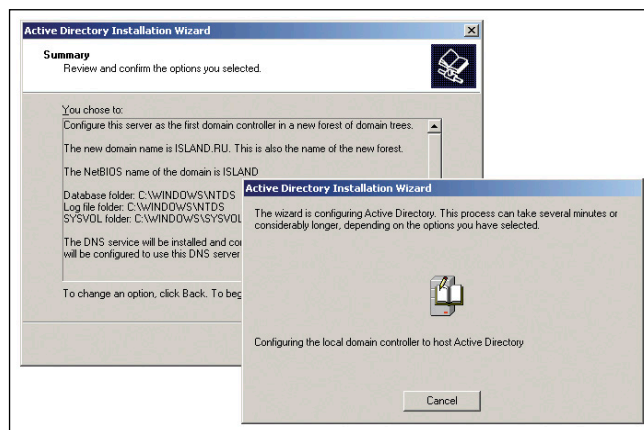


Рисунок 11. Проверка заданных параметров и создание базы Active Directory

На пятом шаге определяют тип создаваемого домена. В файле ответов за тип домена отвечает параметр NewDomain, который принимает одно из трех значений (см. **рис. 5**).

На следующих двух шагах (шестом и седьмом шаге) определяют имя домена и соответствующее ему NetBIOS-имя – сокращенное имя домена (см. **рис. 6**). В файле ответов им соответствуют параметры NewDomainDNSName и NetBIOSName.

На восьмом и девятом шагах указывается физическое расположение базы Active Directory, журнала событий и папки SYSVOL. В файле ответов им соответствуют параметры DataBasePath, LogPath и SysVolPath (см. **рис. 7**). Для создания базы необходимо минимум 200 Мб. Если это условие не будет выполнено, то при создании каталога Active Directory мастер выдаст сообщение об ошибке.

На десятом шаге осуществляется проверка службы DNS и выдается отчет (см. **рис. 8**). В том случае если служба DNS до этого не была установлена и сконфигурирована, это необходимо выполнить как в ручном режиме, так и в автоматическом (рекомендуется). В файле ответов для реализации автоматической настройки необходимо указать значение «Yes» для параметра InstallDNS.

На предпоследнем, одиннадцатом, шаге необходимо выбрать режим работы нового домена. С помощью этой настройки администратор определяет, будет ли совместим создающийся домен с доменами на основе Windows NT. По умолчанию выбран второй вариант (см. **рис. 9**), в котором эта поддержка обеспечена. В файле ответов это

обеспечивается с помощью параметров ForestLevel и DomainLevel.

На завершающем, двенадцатом, шаге необходимо ввести пароль, который будет использован в случае неполадок для входа в режим восстановления домена (см. **рис. 10**). В файле ответов за это отвечает параметр SafeModeAdminPassword.

Не рекомендуется назначать какой-либо пароль, поскольку он будет храниться в незашифрованном виде. После установки необходимо назначить безопасный пароль, поскольку доступ к контроллеру домена необходимо ограничить.

После того как все шаги пройдены, мастер выводит диалоговое окно, в котором администратор может проверить всю введенную информацию. После нажатия на кнопку «Next» осуществляется создание базы Active Directory (см. **рис. 11**). Когда весь процесс завершен, мастер выведет сообщение об успешном создании домена.

После завершения установки и настройки Active Directory выводится соответствующее предложение, затем – предложение перезагрузиться (см. **рис. 12**), чтобы все сделанные изменения вступили в силу.

Отличия работы мастера в Windows 2008 Server

В Windows 2008 Server появилось несколько существенных отличий. Работа мастера значительно переработана и упрощена. К отличиям, которые видны с первого взгляда, относятся следующие:

- Шаги четыре и пять объединены в один.
- NetBIOS-имя домена определяется из заданного DNS-имени, таким образом, седьмой шаг (см. **рис. 6**) исключается.

Все остальные шаги остались без изменений за исключением проверки настройки DNS-сервера и сетевой карты – эти два шага перенесены в самый конец работы мастера. Напомню, что эти оба шага появляются только в случае обнаружения соответствующих неполадок. 🔄

1. RFC 1035. Domain names – implementation and specification.
2. RFC 1123. Requirements for Internet Hosts – Application and Support.
3. RFC 2181. Clarifications to the DNS Specification.

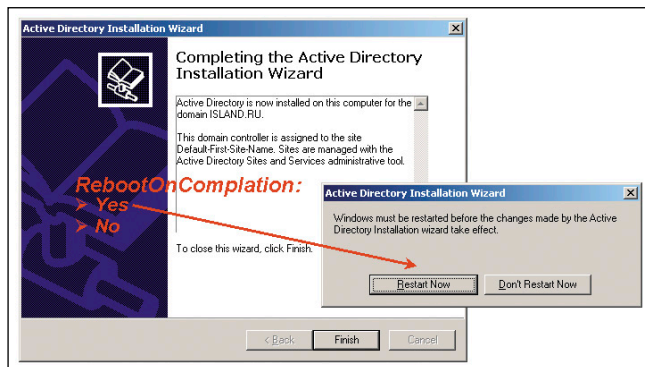


Рисунок 12. Завершение работы мастера настройки Active Directory