**Практическая работа № 3.**

**Тема:** «Установка и настройка Active Directory».

**Цель работы:** приобретение практических навыков установки и настройки Active Directory.

Результаты выполнения практических работ оформляются в виде отчёта. Отчёт должен содержать название и цель работы, краткие теоретические сведения, скриншоты, описания пошагового выполнения практической работы и вывод.

Для защиты практической работы необходимо представить отчёт, оформленный в соответствии с изложенными в методических указаниях требованиями, владеть теоретическим материалом.

**Теоретическая часть.**

Общие сведения.

Каталог представляет собой иерархическую структуру, которая хранит сведения об объектах в сети. Служба каталогов, такая как Active Directory, обеспечивает возможность хранения данных каталога и доступа к этим данным сетевых пользователей и администраторов. Например, в Active Directory хранятся сведения об учетных записях пользователей, такие как имена, пароли, номера телефонов и тому подобные, к которым могут получать доступ другие пользователи той же сети, прошедшие проверку.

Служба каталогов - одна из наиболее важных составных частей развитой компьютерной системы. Пользователи и администраторы зачастую не знают точных имен нужных им объектов, которые им в данный момент требуются. Они могут знать один или несколько их признаков или атрибутов (attributes) и могут послать запрос (query) к каталогу, получив в ответ список тех объектов, атрибуты которых совпадают с указанными в запросе. Служба каталогов позволяет найти любой объект по одному из его атрибутов.

Служба каталогов Active Directory может быть установлена на серверах, работающих под управлением операционных систем Microsoft Windows Server 2003, Standard Edition, Windows Server 2003, Enterprise Edition и Windows Server 2003, Datacenter Edition. Она хранит сведения об объектах сети и упрощает поиск и использование этих сведений пользователям и администраторами. В Active Directory основой для логической, иерархической организации сведений каталога служит структурированное хранилище данных. Это хранилище данных, называемое также каталогом, содержит сведения об объектах Active Directory. В число этих объектов обычно входят общие ресурсы, такие как серверы, тома, принтеры, а также учетные записи сетевых пользователей и компьютеров.

Служба каталогов позволяет обеспечивать защиту информации от вмешательства посторонних лиц в рамках, установленных администратором системы. Группа безопасности интегрирована с Active Directory посредством проверки подлинности при входе в сеть и управления доступом к объектам в каталоге. В рамках одного входа в сеть администраторы могут управлять данными каталога и организацией через их сеть, а прошедшие проверку сетевые пользователи могут иметь доступ к ресурсам во всей сети. Администрирование, основанное на политике, облегчает управление даже самой сложной сетью.

В состав службы Active Directory входят также следующие элементы:

* Набор правил - схему, определяющую классы объектов и атрибуты, содержащиеся в каталоге, а также пределы и ограничения на экземпляры этих объектов, и формат их имен.
* Глобальный каталог, содержащий сведения о каждом объекте в каталоге. Это позволяет пользователям и администраторам находить сведения каталога независимо от того, в каком из доменов каталог в действительности содержатся эти данные.
* Механизм запросов и индексации, позволяющий опубликовывать и находить объекты и их свойства сетевым пользователям или приложениям.
* Службу репликации (тиражирования), распространяющую данные каталога по сети. Все контроллеры домена в домене участвуют в репликации и содержат полную копию всех сведений каталога для своего домена. Любое изменение данных каталога реплицируется во все контроллеры домена в домене.
* Поддержка для программного обеспечения клиента Active Directory, которая предоставляет многие возможности Microsoft Windows 2000 Professional или Windows XP Professional компьютерам, работающих под управлением операционных систем Windows 95, Windows 98 и Windows NT® Server 4.0. Для клиентских компьютеров без клиентского программного обеспечения Active Directory каталог будет выглядеть как каталог Windows NT.

Определим основные понятия, используемые для описания Active Directory.

Область действия (scope) Active Directory достаточно обширна. Она может включать отдельные сетевые объекты (принтеры, файлы, имена пользователей), серверы и домены в отдельной глобальной сети. Она может также охватывать несколько объединенных сетей.

Active Directory, как и любая другая служба каталогов, является, прежде всего, пространством имен. Пространство имен - это такая ограниченная область, в которой может быть распознано данное имя. Распознавание имени заключается в его сопоставлении с некоторым объектом или объемом информации, которому это имя соответствует. Файловая система Windows образует пространство имен, в котором имя файла может быть поставлено в соответствие конкретному файлу. Active Directory образует пространство имен, в котором имя объекта в каталоге может быть поставлено в соответствие самому этому объекту.

Объект - это непустой, именованный набор атрибутов, обозначающий нечто конкретное, например, пользователя, принтер или приложение. Атрибуты содержат информацию, однозначно описывающую данный объект. Атрибуты пользователя могут включать имя пользователя, его фамилию и адрес электронной почты.

Контейнер аналогичен объекту в том смысле, что он также имеет атрибуты и принадлежит пространству имен. Однако, в отличие от объекта, контейнер не обозначает ничего конкретного - он может содержать группу объектов или другие контейнеры.

Термин дерево используется для описания иерархии объектов и контейнеров. Как правило, конечными элементами дерева являются объекты. В узлах (точках ветвления) дерева располагаются контейнеры. Дерево отражает взаимосвязь между объектами или указывает путь от одного объекта к другому. Простой каталог представляет собой контейнер. Компьютерная сеть или домен тоже являются контейнерами.

Домен - это единая область, в пределах которой обеспечивается безопасность данных в компьютерной сети под управлением ОС Windows Server 2003. Active Directory состоит из одного или нескольких доменов. Применительно к отдельной рабочей станции доменом является сама рабочая станция. Границы одного домена могут охватывать более чем одно физическое устройство. Каждый домен может иметь свои правила защиты информации и правила взаимодействия с другими доменами. Если несколько доменов связаны друг с другом доверительными отношениями и имеют единую логическую структуру, конфигурацию и глобальный каталог, то говорят о дереве доменов. Несколько доменных деревьев могут быть объединены в лес.

Дерево доменов (дерево) состоит из нескольких доменов, которые имеют общую логическую структуру и конфигурацию и образуют непрерывное пространство имен. Домены в дереве связаны между собой доверительными отношениями. Active Directory является множеством, которому принадлежат одно или несколько деревьев.

Лесом называется одно или несколько деревьев, которые не образуют непрерывного пространства имен. Все деревья одного леса имеют общие логическую структуру, конфигурацию и глобальный каталог. В отличие от дерева, лес может не иметь какого-то определенного имени.

Узлом называется такой элемент сети, который содержит серверы Active Directory. Узел обычно определяется как одна или несколько подсетей, поддерживающих протокол TCP/IP и характеризующихся хорошим качеством связи. "Хорошее" качество связи в данном случае подразумевает высокую надежность и скорость передачи данных. Определение узла как совокупности подсетей позволяет администратору быстро и без больших затрат настроить топологию доступа и репликации в Active Directory и полнее использовать достоинства физического расположения устройств в сети. Когда пользователь входит в систему, клиент Active Directory ищет серверы Active Directory, расположенные в узле пользователя. Поскольку компьютеры, принадлежащие к одному узлу, в масштабах сети можно считать расположенными близко друг к другу, связь между ними должна быть быстрой, надежной и эффективной. Распознавание локального узла в момент входа в систему не составляет труда, так как рабочая станция пользователя уже знает, в какой из подсетей TCP/IP она находится, а подсети напрямую соответствуют узлам Active Directory.

В Windows Server 2003 Active Directory может быть интегрирована с DNS воедино. DNS представляет собой распределенное пространство имен, которое используется в Интернет и в котором именам отдельных компьютеров и служб ставятся в соответствие адреса, формируемые по правилам протокола TCP/IP. При создании контроллера домена, то есть сервера, управляющего работой Active Directory, мастер предлагает создать и настроить DNS-сервер. В этом случае запускается DNS-сервер и создается зона (контейнер, объединяющий несколько доменов в структуру с общими разрешениями на управление), одноименная с доменом.

Контроллеры домена хранят данные и управляют взаимодействием пользователей с доменом, включая процесс входа в домен, проверку подлинности и поиск в каталогах. Чтобы предоставить сетевым пользователям и компьютерам службу каталогов Active Directory, нужно настроить данный сервер как контроллер домена.

**Практическая часть.**

Для настройки сервера в качестве контроллера домена необходимо установить на данный сервер Active Directory. В мастере установки Active Directory доступны четыре параметра: можно создать дополнительный контроллер домена в существующем домене, контроллер домена для нового дочернего домена, контроллер домена для нового доменного дерева или новый контроллер домена для нового леса. Рассмотрим создание контроллера домена для нового леса.

Операционная система Windows Server 2003 позволяет настроить данный сервер как контроллер домена. Для этого нам необходимо выполнить следующие действия: открыть оснастку "Управление данным сервером"; выбрать ссылку "Добавить или удалить роль"; на странице "Предварительные шаги" прочитать информацию о сетевых соединениях и подтвердить, что все они доступны; на странице "Параметры настройки" выбрать вариант "Особая конфигурация".

На экран будет выведена новая страница, представленная на рис. 1 - Роль сервера.

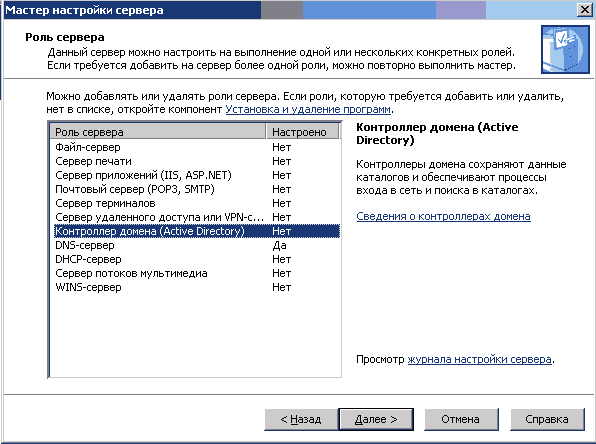


Рис. 1. Роль сервера

На этой странице мы выбираем из приведённого списка "Контроллер домена (Active Directory)" и нажимаем кнопку "Далее".

Появится страница "Сводка выбранных параметров" (рис. 2), в которой можно просмотреть и подтвердить выбранные параметры:

Для применения параметров, выбранных на странице "Сводка выбранных параметров", нажимаем кнопку "Далее".

Появится страница "Применение выбранных параметров", которая будет находиться на экране всё время до окончания установки и настройки Active Directory.

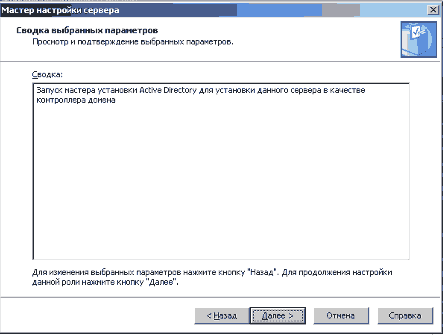


Рис. 2. Сводка выбранных параметров

Автоматически запустится мастер установки Active Directory.

Нажимаем кнопку "Далее" для продолжения. К этой странице можно вернуться из любого места мастера, пока не нажата кнопка "Готово" на последней странице.

Мастер установки выведет на экран страницу, представленную на рис. 3, "Совместимость операционных систем", в которой приводится информация о влиянии усовершенствованных параметров безопасности в Windows Server 2003 на совместимость с предыдущими версиями Windows.

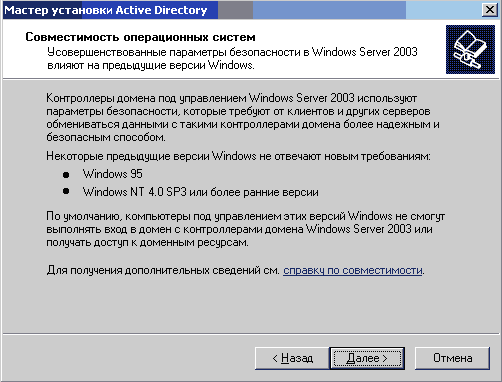


Рис. 3. Совместимость операционных систем

Прочитав сведения, приведённые на этой странице, нажимаем кнопку "Далее".

На странице "Тип контроллера домена" выбираем вариант "Контроллер домена в новом домене" (рис. 4).

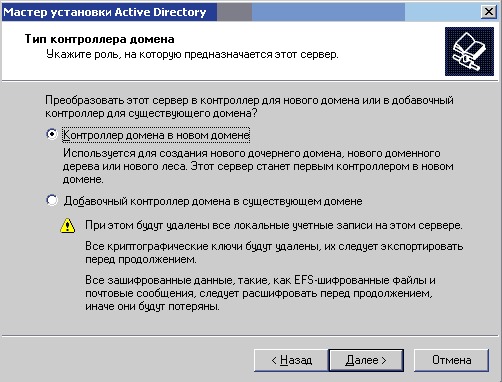


Рис. 4. Тип контролера домена

Для продолжения нажимаем кнопку "Далее".

На появившейся странице, представленной на рис. 5, "Создать новый домен" выбираем вариант "Новый домен в новом лесу".

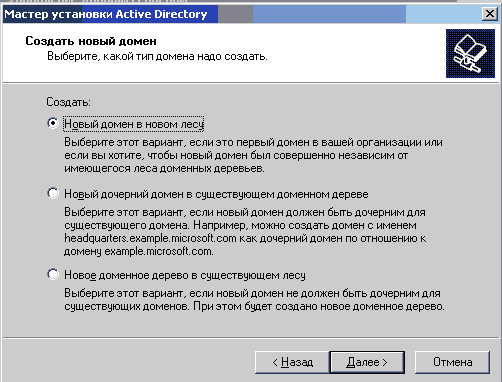


Рис. 5. Тип контролера домена

Для продолжения нажимаем кнопку "Далее". На странице "Новое имя домена" (рисунок 6) вводим полное DNS-имя нового домена.

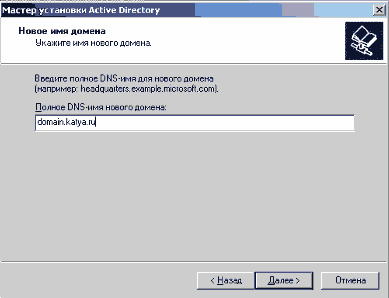


Рис. 6. Новое имя домена

Полное DNS-имя также называют полным доменным именем (FQDN). Домены Active Directory обозначаются с помощью DNS-имен и повторяют иерархическую структуру DNS. DNS-имена для леса Active Directory должны начинаться с зарегистрированного суффикса домена DNS, который зарезервирован организацией для использования в Интернете, например, microsoft.com. Для продолжения нажимаем кнопку "Далее".

На странице NetBIOS-имя домена проверяем NetBIOS-имя, которое будет использоваться пользователями предыдущих версий Windows для идентификации домена (рис. 7).

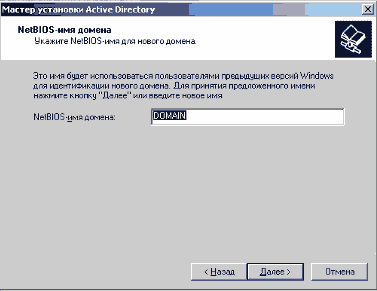


Рис. 7. NetBIOS-имя домена

Домены Active Directory обозначаются в соответствии со стандартами именования DNS, однако при создании доменов Active Directory необходимо задать также NetBIOS-имя. NetBIOS-имена по возможности должны совпадать с первой меткой DNS-имени домена. Если первая метка DNS-имени домена Active Directory отличается от его NetBIOS-имени, в качестве полного доменного имени используется DNS-имя, а не NetBIOS-имя. Например, если первая метка полного DNS-имени домена - child (child.microsoft.com), а NetBIOS-имя домена - sales, полным доменным именем будет child.microsoft.com. Для продолжения нажимаем кнопку "Далее". На странице "Папки базы данных и журналов", представленной на рис. 8, вводим расположение, в которое нужно установить папки базы данных и журналов (или нажимаем кнопку Обзор, чтобы указать расположение).

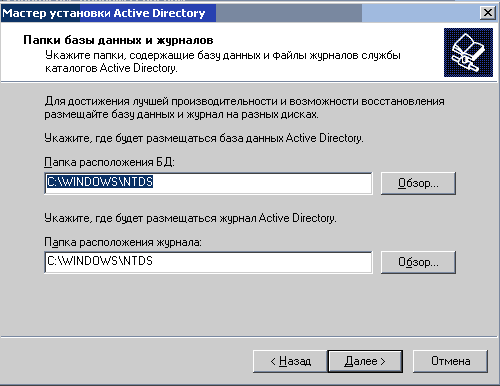


Рис. 8. Папки базы данных и журналов

При этом нужно убедиться, что на диске достаточно места для размещения базы данных каталога и файлов журналов, чтобы избежать проблем при установке или удалении Active Directory. Мастеру установки Active Directory необходимо 250 МБ дискового пространства для установки базы данных Active Directory и 50 МБ для файлов журналов. Рекомендуется размещать данные файлы в разделе NTFS. Для продолжения нажимаем кнопку "Далее".

На странице "Общий доступ к системному тому" (рис. 9) указываем расположение, в которое следует установить папку Sysvol (или нажимаем кнопку Обзор, чтобы указать расположение).

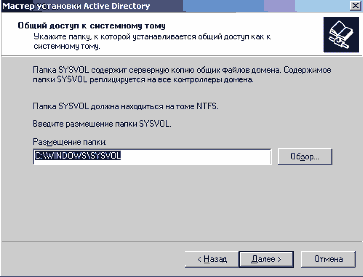


Рис. 9. Общий доступ к системному тому

Папка Sysvol должна находиться в томе NTFS, так как в ней находятся файлы, реплицируемые между контроллерами домена в домене или лесу. Эти файлы содержат сценарии, системные политики для Windows NT 4.0 и более ранних версий, общие папки NETLOGON и SYSVOL и параметры групповой политики. Для продолжения нажимаем кнопку "Далее". На странице "Диагностика регистрации DNS" (рис. 10) проверяем правильность установки параметров.

Если в окне "Результаты диагностики" отображается сообщение об ошибках диагностики, можно нажать кнопку "Справка" для получения дополнительных инструкций по устранению ошибки. Для продолжения нажимаем кнопку "Далее".

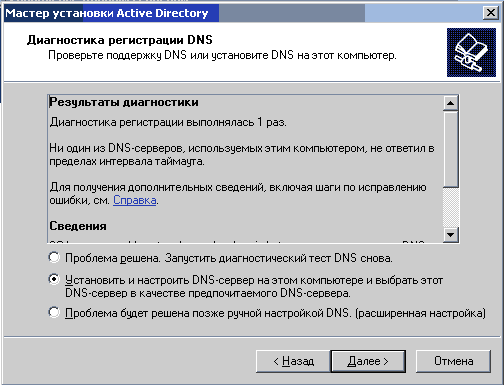


Рис. 10. Диагностика регистрации DNS

На странице "Разрешения" (рис. 11) выбираем требуемый уровень совместимости приложений с операционными системами пред-Windows 2000, Windows 2000 или Windows Server 2003.

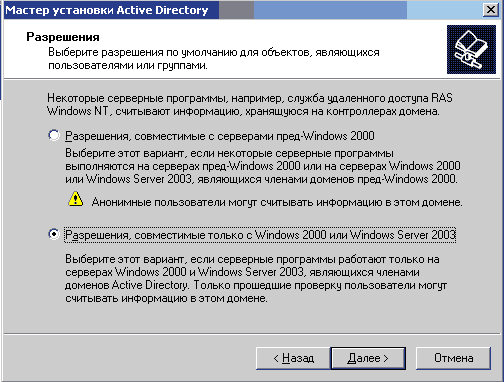


Рис. 11. Выбор требуемого уровня совместимости

На серверах под управлением Windows NT 4.0 и более ранних версий доступ на чтение сведений о пользователях и группах открыт для анонимных пользователей, так что существующие приложения, в том числе Microsoft BackOffice, SQL Server и некоторые приложения других производителей, работают правильно. В Windows 2000 и системах семейства Windows Server 2003 члены группы "Анонимный вход" имеют доступ на чтение к этим сведениям, только если они включены в группу "Пред-Windows 2000 доступ". Для того чтобы добавить группы "Анонимный вход" и "Все" в группу "Пред-Windows 2000 доступ" нужно выбрать вариант "Разрешения, совместимые с серверами пред-Windows 2000". Для того чтобы запретить доступ на чтение сведений о пользователях и группах членам группы "Анонимный вход" мы выбираем вариант "Разрешения, совместимые только с серверами Windows 2000 или Windows Server 2003".

После выбора одного из вариантов можно вручную переключаться между обратной совместимостью и высоким уровнем безопасности объектов Active Directory. Для этого нужно открыть компонент "Active Directory - пользователи и компьютеры" и добавить группу безопасности "Анонимный вход" в группу безопасности "Пред-Windows 2000 доступ". Для продолжения нажимаем кнопку "Далее".

На странице "Пароль администратора для режима восстановления" (рис. 12) нужно ввести и подтвердить пароль для учетной записи администратора режима восстановления для данного сервера.

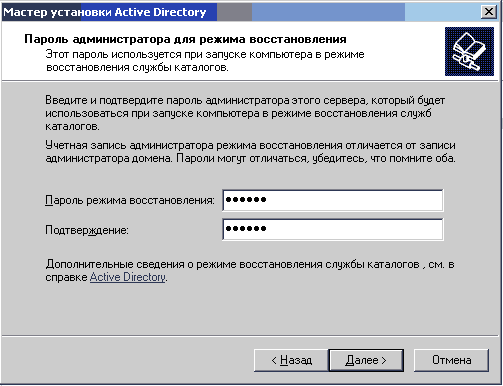


Рис. 12. Пароль администратора для режима восстановления

В качестве паролей режима восстановления каталогов необходимо использовать надежные пароли. Этот пароль необходимо знать для восстановления резервной копии состояния системы данного контроллера домена. Данный пароль нужно также использовать при запуске контроллера домена в режиме восстановления служб каталогов. Для продолжения нажимаем кнопку "Далее".

После этого просматриваем сведения на странице "Сводка", представленной на рис. 13, и нажимаем кнопку "Далее".

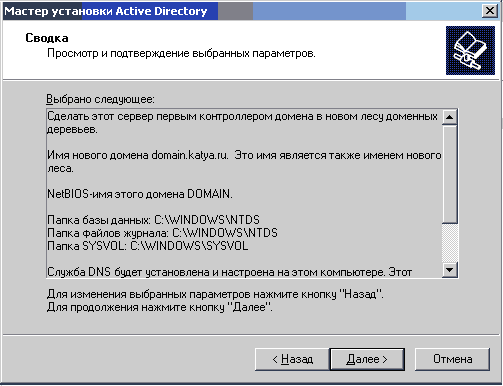


Рис. 13. Просмотр и подтверждения выбранных параметров

Мастер установки настроит Active Directory: После завершения установки нажимаем кнопку "Готово". Для перезагрузки компьютера нажимаем кнопку "Перезагрузить сейчас", чтобы изменения вступили в силу.

После перезагрузки сервера "Мастер настройки сервера" отобразит страницу "Этот сервер теперь является контроллером домена" (рис. 14).

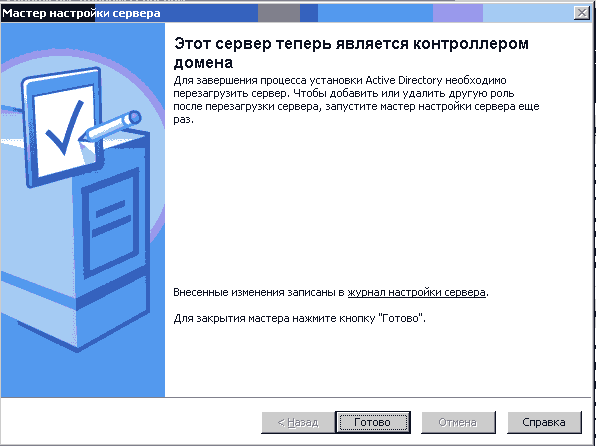


Рис. 14. Подтверждение контроллера домена

Основные средства администрирования домена доступны через главное меню сервера в разделе Администрирование. В повседневной работе администратора наиболее часто используется пункт «Active Directory– пользователи и компьютеры», отмеченный на рисунке 15.

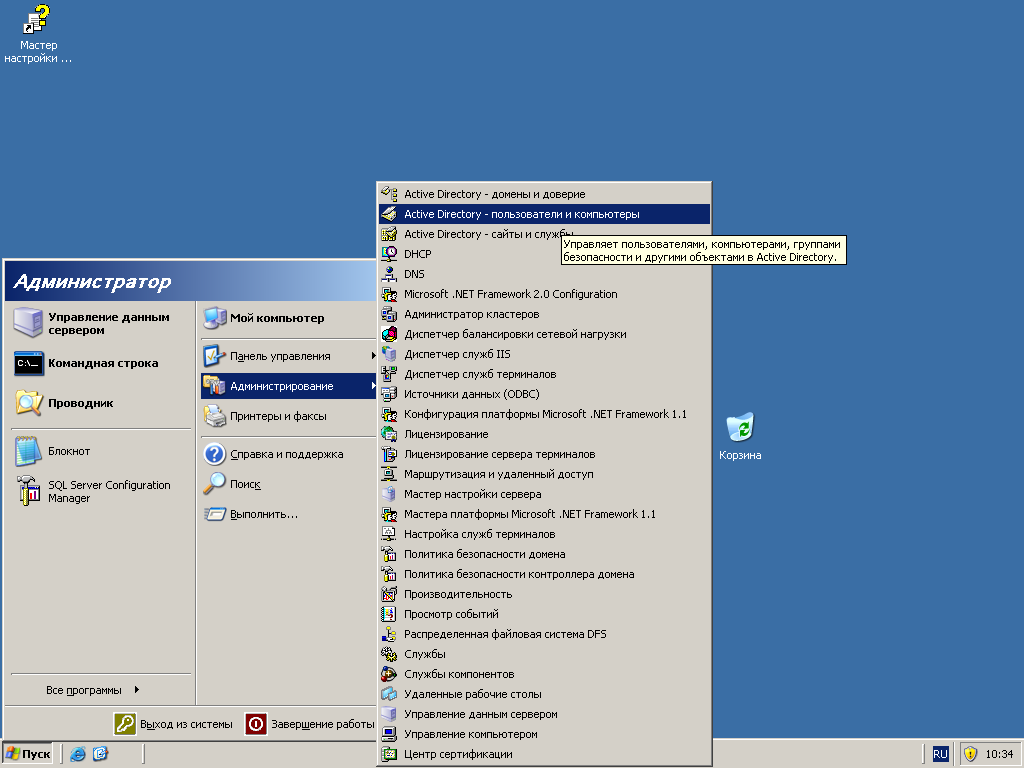


Рисунок 15. Раздел «Администрирование» домена

Следующей задачей создания сети предприятия, позволяющей изучать операционные системы в среде, моделирующей реальную сеть предприятия с правами администратора масштаба предприятия, является подключение компьютера клиента к домену.

Для этого на машине клиента необходимо раскрыть Мой компьютер/Свойства и выбрать раздел «Имя компьютера/Изменение имени компьютера». В этом пункте необходимо выбрать подключение к домену и набрать имя домена и ввести учетную запись администратора домена.

Если все настройки были верными, через некоторое время последует сообщение «Добро пожаловать в домен class.pi» (рисунок 16).

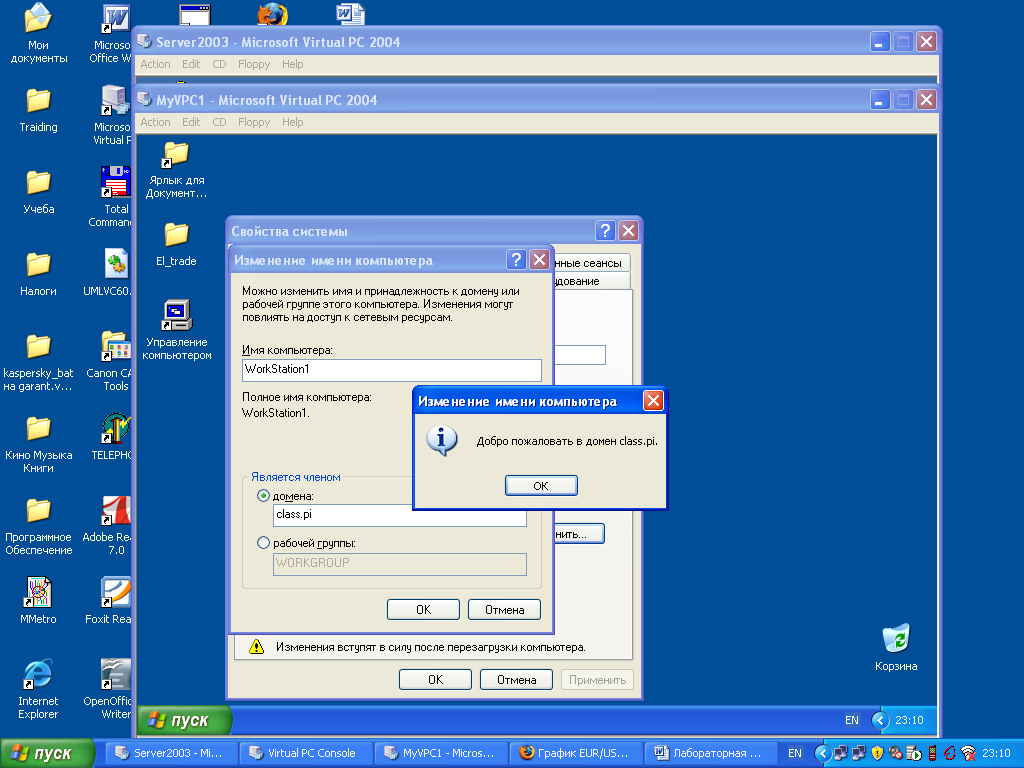


Рисунок 16. Сообщение об успешном подключении к домену

После перезагрузки компьютера становится возможным вход в домен с учетной записью администратора домена, после чего необходимо средствами администрирования сервера приступить к созданию рабочей среды домена

**Задание к проведению практической работы:**

1. Установить службу Active Directory на виртуальном компьютере с операционной системой Windows Server c интегрированной службой DNS. С целью коллективного использования системы в учебном процессе строго выполнить следующее указание: при создании домена установить учетную запись администратора со следующими параметрами: имя – администратор, пароль – **p@ssw0rd**. Создав домен, учащиеся могут создать удобную для себя дополнительную учетную запись с правами администратора.
2. Подключить рабочую станцию к домену, используя учетную запись администратора домена.
3. Продемонстрировать преподавателю полученные результаты и сохранить снимки экранов с основными этапами работы для включения их в отчет о практической работе.

**Контрольные вопросы**

1. С какой целью создается домен?
2. Укажите основные этапы установки Active Directory.
3. Какая ОС должна быть установлена на компьютере, что бы была возможна установка Active Directory?
4. Кто имеет право подсоединить компьютер к домену?
5. Какова роль службы DNS в домене?
6. Почему безопасность системы на основе домена существенно выше, чем в одноранговой сети?
7. Где хранятся учетные записи пользователей и компьютеров домена?
8. В чем отличие учетных записей домена от локальных учетных записей компьютеров одноранговой сети?
9. Если на компьютере установлены протоколы TCP/IP, какую максимальную длину имени компьютера можно задать во время установки?
10. Можно ли изменить имя компьютера после установки ОС на клиентской машине и на контроллере домена?
11. Какое из следующих утверждений верно:
    1. Вы можете подключить компьютер к рабочей группе или домену только во время установки;
    2. Если вы подключите компьютер к рабочей группе во время установки, то к домену можно подключиться позже;
    3. Если вы подключите компьютер во время установки к домену, то к рабочей группе можно подключиться позже;
    4. Вы не можете подключить компьютер к рабочей группе или домену во время установки.