МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для студентов специальности 09.03.04 Программная инженерия
Профиль Разработка и сопровождение программного обеспечения

Ставрополь, 2026

Содержание

Лабораторная работа 1. Установка и настройка сервера DNS

Цель: научиться устанавливать сервер имён, добавлять зоны расширения имён, включать автоматическое обновление зон.

Средства для выполнения работы:

• аппаратные: компьютер с установленной ОС Windows XP.

• программные: приложение ВМ: VirtualBox; виртуальные машины: VM-1, VM-2; установочные образы ОС: winXP.iso.

Теоретические сведения

*Система доменных имен (**DNS**)* была исходно определена в документах **RFC (*Request for Comments*) 1034 и 1035**. Эти документы определяют следующие элементы, общие для всех реализаций программного обеспечения ***DNS***.

• Пространство доменных имен ***DNS***, которое задает структурированную иерархию доменов, используемую для организации имен.

• Записи ресурсов, сопоставляющие доменные имена ***DNS*** определенным типам информации о ресурсах, которые используются при регистрации и разрешении имен в пространстве имен.

• ***DNS***-серверы, которые сохраняют записи ресурсов и отвечают на запросы клиентов.

• ***DNS***-клиенты, которые также называют системами разрешения имен, запрашивающие серверы для поиска и разрешения имен по типам записей ресурсов, указанным в запросе.

Пространство доменных имен ***DNS***, как показано на следующем рисунке, базируется на концепции дерева именованных доменов. Каждый уровень дерева может представлять ветвь или лист дерева. Ветвь представляет уровень, на котором используется несколько имен, определяющих семейство именованных ресурсов. Лист представляет единственное имя, которое используется на этом уровне для указания конкретного ресурса.

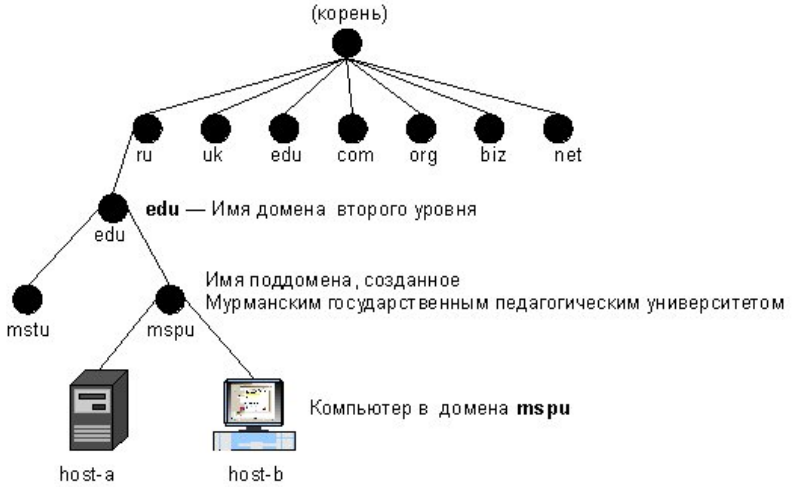

Рисунок 1. Пространство доменных имен.

В процессе разрешения имен существенно, что ***DNS***-серверы часто действуют как ***DNS***-клиенты, запрашивая другие серверы с целью полного разрешения имени в запросе. Любое доменное имя***DNS*** в дереве технически

представляет домен. Однако принято считать что имена идентифицируются одним из пяти способов на основании уровня и способа использования имени.

Тип имени	**Описание**	**Пример**
Корень доменов	Вершина дерева, представляющая неименованный уровень, иногда обозначается парой прямых кавычек (""), указывающих пустое значение. При использовании в доменном имени ***DNS*** для этого применяется завершающая точка (.), свидетельствующая, что имя расположено в корне или на самом верхнем уровне иерархии доменов. В данном случае доменное имя ***DNS*** рассматривается как полное и указывает на точное расположение в дереве имен. Имена, установленные таким способом, называют полными доменными именами (***Fully Qualified Domain Name, FQDN***).	Единственная точка (.) или точка, использованная в конце имени, например,**«example.microsoft.com.»**
Домен верхнего уровня	Имя из двух или трех букв, которое используется, чтобы указать страну/регион или тип организации.	**«.ru»** указывает имя, зарегистрированное для коммерческого использования в Интернете.
Домен второго уровня	Имена переменной длины, зарегистрированные для индивидуальных пользователей или организаций для использования в Интернете. Эти имена всегда базируются на соответствующем домене верхнего уровня в зависимости от типа организации или географического расположения, в котором используется имя.	**«edu.ru.»** является именем домена второго уровня, зарегистрированным для образовательных учреждений регистратором доменных имен***DNS*** Интернета.
Поддомен	Дополнительные имена, которые организация может создавать как производные от зарегистрированного имени домена второго уровня. Такие имена обеспечивают рост дерева имен ***DNS*** в организации и его распределение по отделам или по географическому расположению.	**«mspu.edu.ru»** представляет имя поддомена Мурманского государственного педагогического университета.
Имя узла или ресурса	Имя, представляющее лист в дереве имен ***DNS***, которое определяет конкретный ресурс. Обычно крайняя левая метка в доменном имени ***DNS*** определяет конкретный компьютер в сети. Например, имя этого уровня, используемое в записи ресурса узла (A), используется для поиска IP-	**«host-a.mspu.edu.ru.»**, где первая метка (**«host-a»**) представляет имя узла ***DNS*** для конкретного компьютера в сети.

	адреса компьютера по его имени узла.	

Например, доменное имя ***DNS***, зарегистрированное для образовательных учреждений (**edu.ru.**), представляет домен второго уровня. Это имя состоит из двух частей (называемых метками), показывающих, что оно находится на втором уровне сверху от корня или вершины дерева. Большинство доменных имен ***DNS*** содержат две или большее число меток, каждая из которых задает новый уровень в дереве. Точки используются в именах для разделения меток.

DNS представляет способ интерпретации полного пути к доменному имени ***DNS*** аналогично способу интерпретации полного пути к файлу или каталогу в окне командной строки. Например, путь в дереве каталогов помогает указать на точное расположение файла, сохраненного на компьютере. Для компьютеров с операционной системой **Windows** обратная косая черта (\) указывает каждый новый каталог, ведущий к точному расположению файла. Эквивалентным символом в ***DNS*** является точка (**.**), указывающая каждый новый уровень домена в имени. Для ***DNS*** примером имени с несколькими уровнями может служить следующее полное доменное имя узла: **host-a.mgupi.edu.ru.** В отличие от имен файлов, при чтении полного доменного имени узла ***DNS*** слева направо осуществляется переход от наиболее конкретной информации (имя ***DNS*** компьютера **«host-a»**) к наиболее общей (завершающая точка (**.**), которая указывает корень в дереве имен ***DNS***). Этот пример демонстрирует четыре уровня доменов ***DNS***, которые ведут от конкретного расположения **«host-a»**.

1. Домен **«mspu»**, в котором зарегистрировано для использования имя компьютера **«host-a»**.
2. Домен **«edu»**, который соответствует родительскому домену, являющемуся корнем поддомена **«mgupi»**.
3. Домен **«ru»**, который соответствует домену верхнего уровня, предназначенному для использования организациями из России, который является корнем для домена **«edu»**.
4. Завершающая точка (**.**), представляющая стандартный символ разделителя, которая используется, чтобы сделать полным доменное имя ***DNS*** в дереве пространства имен ***DNS***.

Работа запросов DNS

Когда ***DNS***-клиенту требуется найти имя, используемое в программе, он запрашивает ***DNS***-серверы для сопоставления имени. Каждое сообщение с запросом, отправляемое клиентом, содержит информацию трех типов, определяющую вопрос, на который отвечает сервер:

1. указанное доменное имя ***DNS*** в виде полного доменного имени узла (**FQDN**);
2. указанный тип запроса, в котором задается либо тип записей ресурсов, либо тип операции запроса;
3. указанный класс доменного имени ***DNS***.

Для ***DNS***-серверов **Windows** этот класс всегда должен быть указан как класс Интернета (**IN**).

Например, указанное имя может представлять полное доменное имя узла для компьютера, такое как **«host-a. mgupi.edu.ru.»**, и тип запроса на поиск записей ресурсов адреса (A) для этого имени. Запрос ***DNS*** можно представить как вопрос клиента, состоящий из двух частей, например *«Имеются ли записи ресурсов A для компьютера с именем 'hostname.mgupi.edu.ru.'?»* Когда клиент получает ответ от сервера, он читает и интерпретирует содержащуюся в ответе запись ресурса A, узнавая IP-адрес компьютера, запрошенного по имени.

Запросы ***DNS*** используют несколько способов сопоставления имен. Клиент может иногда ответить на запрос с помощью локальной кэшированной информации, полученной в предыдущем запросе.***DNS***-сервер может использовать собственный кэш информации о записях ресурсов для ответа на запрос. ***DNS*** -сервер может также запросить или обратиться к другим ***DNS***-серверам в интересах запрашивающего клиента для полного сопоставления имени, а затем отправить ответ клиенту. Этот процесс называют *рекурсией*.

В дополнение к этому, клиент может самостоятельно пытаться установить контакт с дополнительными ***DNS***-серверами для сопоставления имени. При этом клиент использует отдельные дополнительные запросы, базирующиеся на ссылочных ответах от серверов. Этот процесс называют *итерацией*. В общем случае процесс запроса ***DNS*** выполняется в две стадии.

1. Запрос к имени начинается на клиентском компьютере и передается в систему сопоставления имен службы ***DNS***-клиент.
2. Когда не удается ответить на запрос на локальном уровне, можно для сопоставления имени запрашивать ***DNS***-серверы по мере необходимости.

Обе стадии процесса подробнее рассматриваются в следующих разделах.

Локальная система разрешения имен

На начальных этапах процесса в программе на локальном компьютере используется доменное имя ***DNS***. Затем запрос передается в службу «***DNS***-клиент» для сопоставления с помощью локальной кэшированной информации. Если удается разрешить запрошенное имя, поступает ответ на запрос и процесс завершается. Кэш локального сопоставления имен может включать информацию об именах из двух возможных источников.

1. Если имеется локальный файл **Hosts**, все сопоставления имен и адресов из этого файла предварительно загружаются в кэш при запуске службы «***DNS***-клиент».
2. Записи ресурсов, полученные в ответах на запросы из предыдущих запросов ***DNS***, добавляются в кэш и сохраняются в нем в течение определенного периода времени.

Если клиент не находит сопоставления в кэше, процесс продолжается с помощью запроса на разрешение имени от клиента к ***DNS***-серверу.

Запрос к DNS-серверу

Клиент запрашивает основной ***DNS***-сервер. Из глобального списка выбирается сервер, используемый на начальной стадии запроса от клиента к серверу. Когда ***DNS***-сервер принимает запрос, он сначала проверяет, можно ли дать удостоверяющий ответ на базе записей ресурсов, содержащихся в

локальной зоне в конфигурации сервера. Если запрошенное имя соответствует информации в записи ресурса в локальной зоне, сервер дает удостоверяющий ответ, используя эту информацию для разрешения имени. Если в зоне нет информации для запрошенного имени, сервер проверяет, можно ли разрешить имя, используя информацию предыдущих запросов в локальном кэше. Если здесь обнаруживается совпадение, сервер отвечает с использованием этой информации. И в этом случае, если основной сервер может дать запрашивающему клиенту утвердительный ответ на сопоставление из собственного кэша, запрос завершается. Если на основном сервере не удается найти запрошенное имя — ни в кэше, ни в зонах — процесс выполнения запроса может продолжаться с использованием рекурсии для полного разрешения имени. При этом другие ***DNS***-серверы помогают разрешить имя. Служба «***DNS***-клиент» по умолчанию указывает серверу использовать процесс рекурсии для полного разрешения имен в интересах клиентов перед возвращением ответа. В большинстве случаев ***DNS***-серверы по умолчанию настраиваются на поддержку процесса рекурсии, как показано на следующем рисунке.

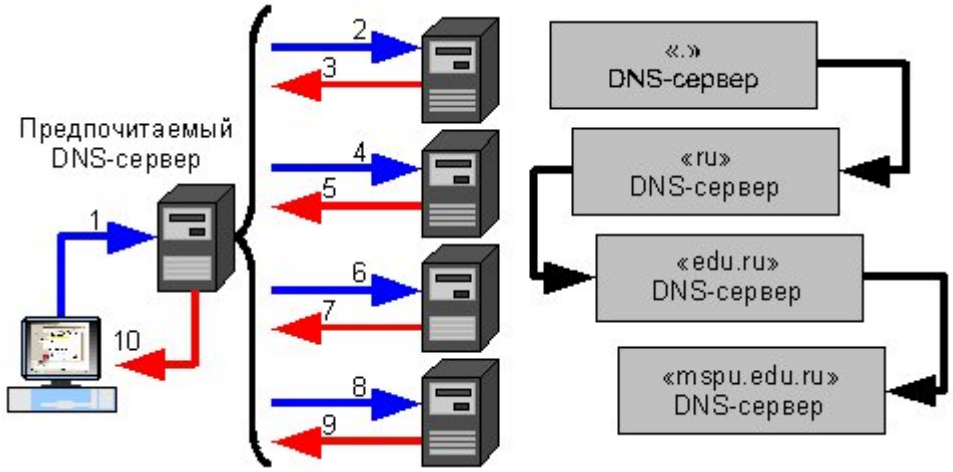

Рисунок 2. Процесс рекурсии при разрешении имени.

Для правильного выполнения рекурсии ***DNS***-сервером ему необходимы сведения о контактах с другими ***DNS***-серверами в пространстве доменных имен ***DNS***. Такая информация обеспечивается в виде корневых ссылок, списка предварительных записей ресурсов, которые могут использоваться службой ***DNS*** для обнаружения других ***DNS***-серверов, которые являются удостоверяющими для корня дерева пространства доменных имен ***DNS*** . Корневые серверы являются удостоверяющими для корня доменов и доменов верхнего уровня в дереве пространства доменных имен ***DNS***.

Ранее отмечалось, что процесс заканчивается возвращением клиенту утвердительного ответа. Однако запросы могут возвращать и другие ответы. Приведем наиболее общие типы таких ответов:

1. удостоверяющий ответ;
2. утвердительный ответ;
3. ссылочный ответ;
4. отрицательный ответ.

Удостоверяющий ответ представляет утвердительный ответ, возвращенный клиенту и доставленный с установленным битом полномочий в сообщении ***DNS***, указывающим, что ответ получен от сервера, имеющего прямые полномочия для запрашиваемого имени.

Утвердительный ответ может содержать запрошенную запись ресурса или список записей ресурсов (который также называют набором записей), соответствующих запрошенному доменному имени ***DNS*** и типу записи, указанному в сообщении запроса.

Ссылочный ответ содержит дополнительные записи ресурсов, не указанные по имени или типу в запросе. Ответ этого типа возвращается клиенту, если процесс рекурсии не поддерживается. Эти записи должны рассматриваться как справочные, которые могут использоваться клиентом для продолжения запроса с помощью итераций. Если клиент способен использовать итерации, он может выполнить дополнительные запросы в попытке полностью разрешить имя самостоятельно.

Отрицательный ответ от сервера может указывать на один из двух возможных результатов попытки сервера обработать и рекурсивно полностью и удостоверяющим образом сопоставить имя в запросе:

- Удостоверяющий сервер ответил, что запрошенное имя не существует в пространстве имен ***DNS***.
- Удостоверяющий сервер ответил, что запрошенное имя существует, но для этого имени отсутствуют записи указанного типа.

Система сопоставления имен передает результаты запроса в виде утвердительного или отрицательного ответа в запрашивающую программу и кэширует ответ. Итерации представляют тип сопоставления имен, используемый ***DNS***-клиентами и серверами при выполнении следующих условий.

- Клиент запрашивает использование рекурсии, но рекурсия отключена на ***DNS***-сервере.
- Клиент не запрашивает использование рекурсии при запросе к ***DNS***-серверу.

Итерационный запрос от клиента сообщает ***DNS***-серверу, что клиент ожидает от ***DNS***-сервера наиболее точный ответ немедленно без обращения к другим ***DNS***-серверам. Когда используются итерации, ***DNS***-сервер отвечает клиенту о запрошенных именах на основании собственной информации о пространстве имен. Например, если ***DNS***-сервер в интрасети получает запрос от локального клиента для имени **«www.edu.ru»**, он может возвратить ответ из кэша имен. Если в данный момент запрошенное имя не сохраняется в кэше сервера, то сервер может ответить предоставлением ссылки — т.е. списка записей ресурсов других ***DNS*** -серверов, которые ближе к имени, запрошенному клиентом. Когда предоставляется ссылка, ***DNS***-клиент принимает на себя ответственность за продолжение итерационных запросов на сопоставление имени к другим указанным в конфигурации ***DNS***-серверам. Например, в наиболее общем случае ***DNS***-клиент может расширить область поиска до серверов корневого домена в Интернете в попытках обнаружить

удостоверяющие ***DNS***-серверы для домена **«ru»**. После установления контакта с корневыми серверами Интернета клиент может получить от них дальнейшие итерационные ответы, указывающие на фактические ***DNS***-серверы Интернета для домена **«edu.ru»**. Когда клиенту предоставляются записи для этих ***DNS***-серверов, он может отправить дальнейший итерационный запрос внешним ***DNS*** -серверам **edu** в Интернете, которые могут дать определенный и удостоверяющий ответ. При использовании итераций ***DNS***-сервер может также содействовать в запросе на сопоставление имени, предоставив клиенту собственный наиболее точный ответ. Для большинства итерационных запросов клиент использует локальный список ***DNS***-серверов для обращения к другим серверам имен в пространстве имен ***DNS***, если его собственный основной ***DNS***-сервер не может сопоставить имя в запросе.

По мере того как ***DNS***-серверы обрабатывают запросы клиентов с помощью рекурсии или итераций, они находят и накапливают значительный объем информации о пространстве имен ***DNS***. Эта информация *кэшируется* сервером. Кэширование дает возможность ускорить сопоставление часто используемых имен ***DNS*** в последующих запросах и существенно снижает трафик запросов ***DNS*** в сети. При выполнении рекурсивных запросов ***DNS***-серверами для клиентов они временно кэшируют записи ресурсов. Кэшированные записи ресурсов содержат информацию, полученную от ***DNS***-серверов, которые являются удостоверяющими для доменных имен ***DNS***. Эта информация накапливается при выполнении итерационных запросов в процессе поиска и полного ответа на рекурсивный запрос, выполняемый в интересах клиента. Когда затем другие клиенты размещают новые запросы на информацию, отвечающую кэшированным записям ресурсов, ***DNS***-сервер может использовать данные из кэшированных записей ресурсов для ответа. При кэшировании информации значение срока жизни применяется ко всем кэшированным записям ресурсов. Пока не истек срок жизни кэшированной записи ресурса, ***DNS***-сервер может продолжать кэшировать и снова использовать запись ресурса при ответах на соответствующие запросы клиентов. Значения срока жизни кэширования, используемые записями ресурсов в большинстве конфигураций зон, назначаются в параметре **Мин. срок жизни TTL (по умолчанию)**, который задается в начальной записи зоны. По умолчанию задается значение минимального срока жизни 3600 секунд (1 час), но это значение может быть изменено; могут также задаваться отдельные значения срока жизни для каждой записи ресурса.

Обратный просмотр

В большинстве операций просмотра ***DNS***-клиенты обычно выполняют *прямой просмотр*, т. е. поиск, основанный на имени ***DNS*** другого компьютера, сохраненного в записи ресурса адреса (A). В этом типе запроса в качестве данных для ответа на запрос ожидается IP-адрес. ***DNS*** также обеспечивает возможность *обратного просмотра*, в котором клиенты используют известный IP-адрес для поиска имени компьютера по этому адресу.

Обратный просмотр фактически является формой вопроса типа «Можете ли вы сказать мне имя ***DNS*** компьютера, который использует IP-адрес 192.168.1.20?».

Система ***DNS*** не разрабатывалась изначально для поддержки запросов этого типа. Одной из проблем при поддержке запросов обратного просмотра является различие в способах организации и индексации пространства имен ***DNS*** и способов назначения IP-адресов. Если бы единственным таким способом был бы поиск во всех доменах пространства имен ***DNS***, то для обработки обратного запроса потребовалось бы слишком много времени и такой запрос оказался бы бесполезным.

Чтобы разрешить эту проблему, в стандартах ***DNS*** был определен и зарезервирован специальный домен в пространстве имен ***DNS*** Интернета, **in-addr.arpa**, обеспечивающий практичный и надежный способ выполнения обратных запросов. Чтобы создать обратное пространство имен, поддомены в домене **in-addr.arpa** формируются с помощью обратного упорядочения чисел в точечно-десятичной нотации IP-адресов. Такое обратное упорядочение доменов для каждого октета необходимо, поскольку в отличие от имен ***DNS***, для которых IP-адреса читаются слева направо, здесь интерпретация выполняется в обратном порядке. Когда IP-адрес читается слева направо, информация анализируется от наиболее общей (IP-адрес сети в левой части адреса) до наиболее конкретной (IP-адрес узла в последнем октете). По этой причине порядок октетов IP-адреса должен быть обращен при построении дерева домена **in-addr.arpa**. IP-адреса дерева ***DNS*** **in-addr.arpa** могут делегироваться организациям, которым назначается ограниченный набор IP-адресов в границах определенных для Интернета классов адресов. И, наконец, для дерева домена **in-addr.arpa**, встроенного в ***DNS***, требуется определение дополнительного типа записей ресурсов — запись ресурса указателя (**PTR**). Такая запись ресурса используется для сопоставления в зоне обратного просмотра, обычно соответствующего записи ресурса именованного узла (A) для имени ***DNS*** компьютера в зоне прямого просмотра.

Следующий рисунок иллюстрирует обратный запрос, инициируемый ***DNS***-клиентом (**host-b**), которому требуется узнать имя другого узла (**host-a**) поего IP-адресу 192.168.1.20.

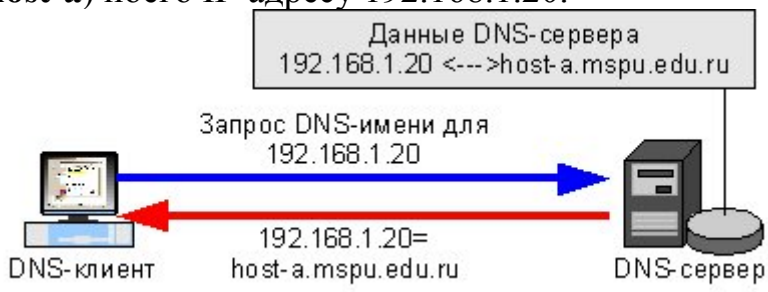

Рисунок 3. Обратный запрос.

Как показано на рисунке, обратный запрос включает следующие этапы.

1. Клиент **«host-b»** запрашивает ***DNS***-сервер о записи ресурса указателя (**PTR**), сопоставляющей IP-адрес 192.168.1.20 для имени **«host-a»**. *Поскольку запрос относится к записям* ***PTR****, система сопоставления имен обращает адрес и добавляет имя домена* ***«in-addr.arpa»*** *в конец обращенного*

*адреса. В результате образуется полное доменное имя узла (**«20.1.168.192.in-addr.arpa.»**), для которого будет проводиться поиск в зоне обратного просмотра.*

2. После обнаружения имени удостоверяющий ***DNS***-сервер для имени **«20.1.168.192.in-addr.arpa»** может возвратить ответ с информацией записи **PTR**. В этой информации содержится доменное имя***DNS*** узла **«host-a»**, что приводит к завершению процесса обратного просмотра. *Необходимо помнить, что если запрошенное обратное имя не может быть возвращено **DNS**-сервером, можно использовать сопоставление имен **DNS** (либо рекурсию, либо итерации) для обнаружения **DNS**-сервера, который является удостоверяющим для зоны обратного просмотра и содержит запрашиваемое имя. В этом смысле процесс сопоставления имен при обратном просмотре аналогичен процессу прямого просмотра*

Инвертированные запросы

Инвертированные запросы являются устаревшим средством, которое ранее было предложено как часть стандарта ***DNS*** для поиска имени узла поего IP-адресу. В них используются нестандартные операции запросов ***DNS***, а их применение ограничено ранними версиями программы **Nslookup**, которая является утилитой командной строки для устранения неполадок и тестирования службы ***DNS***.

Служба ***DNS*** распознает и принимает сообщения инвертированных запросов и отвечает на них с имитацией ответа на инвертированный запрос.

Динамическое обновление

Динамическое обновление позволяет компьютерам ***DNS***-клиентов регистрировать и динамически обновлять собственные записи ресурсов с помощью ***DNS***-сервера при каждом возникновении изменений. Это снижает необходимость администрирования записей зон вручную, в особенности для клиентов, которые путешествуют или часто меняют расположение и получают IP-адреса через ***DHCP***.

Клиентские и серверные службы ***DNS*** поддерживают использование динамических обновлений, как описано в документе ***RFC 2136, «Dynamic Updates in the Domain Name System»***. Служба ***DNS***-сервер поддерживает включение и отключение динамических обновлений отдельно для каждой зоны на каждом сервере, настроенном для загрузки либо стандартной основной зоны, либо зоны, интегрированной в каталоги. Служба ***DNS***-клиент будет по умолчанию динамически обновлять свои записи ресурсов узла (A) в ***DNS***, когда была выполнена настройка для **TCP/IP**.

Динамические обновления обычно запрашиваются, когда изменяется имя ***DNS*** или IP-адрес компьютера. Например, предположим, что для клиента с именем **«oldhost»** в окне **Свойства системы**заданы следующие имена:

Имя компьютера	oldhost
Доменное DNS-имя компьютера	mgupi.edu.ru.
Полное имя компьютера	oldhost.mgupi.edu.r

	u

Таблица 2. Старые имена компьютера.

В этом примере в конфигурации компьютера нет доменных имен ***DNS***, специфических для подключения. В дальнейшем компьютер переименовывается из **«oldhost»** в **«newhost»**, в результате чего имена изменяются следующим образом.

Имя компьютера	newhost
Доменное DNS-имя компьютера	mgupi.edu.ru.
Полное имя компьютера	mgupi.mspu.edu.ru

Таблица 3. Новые имена компьютера.

После изменения имени в окне **Свойства системы** отображается приглашение перезагрузить компьютер. Когда при перезагрузке компьютер запускает ОС, служба ***DHCP***-клиент выполняет следующие действия для обновления ***DNS***.

1. Служба ***DHCP***-клиент отправляет запрос для типа начальной записи зоны (**SOA**) с использованием доменного имени ***DNS*** компьютера. Клиентский компьютер использует текущее полное доменное имя узла компьютера (в данном случае **«newhost.mgupi.edu.ru»**) как имя, указанное в этом запросе.
2. Удостоверяющий ***DNS***-сервер зоны, содержащей полное доменное имя узла клиента, отвечает на запрос типа **SOA**.
3. После этого служба ***DHCP***-клиент пытается установить контакт с основным ***DNS***-сервером. *Клиент обрабатывает ответ на запрос **SOA** для его имени, чтобы определить IP-адрес **DNS**-сервера, удостоверенного как основной сервер, для принятия его имени. Далее он выполняет такую последовательность шагов, необходимых, чтобы установить контакт и динамически обновить его основной сервер.*

a. Клиент отправляет запрос на динамическое обновление основному серверу, определенному в ответе на запрос **SOA**. *Если обновление выполняется успешно, другие действия не предпринимаются.*

b. При отказе на обновление клиент отправляет запрос типа **NS** (о серверах имен) для зоны, имя которой указано в записи **SOA**.

c. Когда клиент получает ответ на этот запрос, он отправляет запрос **SOA** на первый ***DNS***-сервер, перечисленный в ответе.

d. После разрешения имен в запросе **SOA** клиент отправляет динамическое обновление серверу, указанному в возвращенной записи **SOA**. *Если обновление выполняется успешно, другие действия не предпринимаются.*

e. При отказе на обновление клиент повторяет запрос **SOA**, отправляя его к следующему ***DNS***-серверу, перечисленному в ответе.

4. Как только находится основной сервер, который может выполнить обновление, клиент отправляет запрос на обновление, который обрабатывается сервером.

Содержимое запроса на обновление включает инструкции добавить записи ресурсов A (и возможно **PTR**) для имени **«newhost.mgupi.edu.ru»** и записи этих типов для ранее зарегистрированного имени **«oldhost.mgupi.edu.ru»**.

Сервер также выполняет проверку, разрешены ли обновления для запроса клиента. Для стандартных основных зон динамические обновления не являются безопасными, поэтому для клиентов должны выполняться любые попытки обновления. Для зон, интегрированных в службу каталогов ***Active Directory***, обновления являются безопасными и выполняются с помощью параметров безопасности, устанавливаемых на основе каталогов.

Динамические обновления отправляются или выполняются периодически. По умолчанию компьютер отправляет обновления каждые 7 дней. Если в результате обновления данные в зоне не изменяются, зона остается в текущей версии и никакие изменения не записываются. Обновления выполняются только при фактических изменениях имен и адресов в зоне или в результате добавочной зонной передачи.

Безопасное динамическое обновление

Безопасные обновления ***DNS*** доступны только для зон, интегрированных в службу каталогов ***Active Directory***. После преобразования зоны в интегрированную становится возможным использование с консоли ***DNS*** списков управления доступом. Можно добавлять пользователей и группы в списки или удалять их для указанной зоны или записи ресурса. Параметры безопасного динамического обновления для ***DNS***-серверов и клиентов по умолчанию обрабатываются следующим образом.

• ***DNS***-клиенты сначала предпринимают попытки выполнить небезопасные динамические обновления. При отказе на небезопасные обновления клиенты пытаются выполнить безопасные обновления. *Кроме того, клиенты используют политику обновления по умолчанию, которая позволяет им пытаться переписывать ранее зарегистрированную запись ресурса, если она специально не заблокирована условиями безопасности обновления.*

• После интегрирования зоны в службу каталогов ***Active Directory DNS***-серверам **Windows Server 2003** по умолчанию разрешаются только безопасные динамические обновления.

*При использовании стандартного сохранения зон настройки по умолчанию службы **DNS**-сервер не разрешают динамические обновления зон. И для зон, интегрированных в каталоги, и для использующих стандартное сохранение в файлах можно изменить параметры зоны и разрешить динамические обновления. Это позволяет принимать любые обновления.*

При развертывании ***DNS***-серверов совместно с ***Active Directory*** необходимо иметь в виду следующее:

• Служба ***DNS*** требуется для обнаружения контроллеров доменов **Windows Server 2003**. Служба сетевого входа в систему использует новые средства поддержки ***DNS***-серверов для обеспечения регистрации контроллеров доменов в пространстве доменных имен ***DNS***.

• ***DNS***-серверы **Windows Server 2003** могут использовать службу каталогов ***Active Directory*** для сохранения и репликации зон. *При интегрировании зон в службу каталогов пользователи получают возможность использовать дополнительные средства* ***DNS****, такие как безопасные динамические обновления и средства устаревания и очистки записей.*

Способы интеграции ***DNS*** со службой каталогов ***Active Directory***:

• При установке ***Active Directory*** на сервер выполняется повышение сервера до роли контроллера указанного домена. Когда данный процесс завершается, пользователю выводится приглашение указать доменное имя ***DNS*** для домена ***Active Directory***, для которого выполняется присоединение и повышение сервера.

• Если в этом процессе удостоверяющий ***DNS***-сервер для указанного домена либо не обнаруживается в сети, либо не поддерживает протокол динамического обновления ***DNS***, выводится приглашение установить ***DNS***-сервер. Такая возможность предоставляется, поскольку ***DNS***-серверу необходимо отыскать этот сервер или другие контроллеры домена для рядовых серверов домена***Active Directory***.

После установки ***Active Directory*** имеются две возможности сохранения и репликации зон при работе с ***DNS***-сервером на новом контроллере домена.

• Стандартное сохранение зоны с помощью файла в текстовом формате. *Зоны, сохраняемые в этом способе, размещаются в файлах с раширением* ***DNS****, которые сохраняется в папке* ***systemroot\System32\Dns*** *на каждом компьютере, на котором выполняется* ***DNS****-сервер. Имя файла зоны соответствует имени, которое пользователь выбрал для зоны при ее создании, например,* ***mgupi.edu.ru.dns****, если именем зоны является* ***«mgupi.edu.ru.dns»****.*

• Сохранение зон, интегрированных в службу каталогов, с помощью базы данных ***Active Directory***. *Зоны, сохраняемые таким образом, размещаются в дереве* ***Active Directory*** *под разделом каталога домена или приложения. Каждая зона, интегрированная в службу каталогов, сохраняется в контейнере* ***dnsZone****, который идентифицируется по имени, выбранному пользователем при ее создании.*

Преимущества интеграции с ***Active Directory***

В сетях с развертыванием ***DNS*** для поддержки службы каталогов ***Active Directory*** настоятельно рекомендуется использовать основные зоны, интегрированные в службу каталогов, которые предоставляют следующие преимущества.

• Обновление с несколькими главными серверами и расширенные средства безопасности, базирующиеся на возможностях ***Active Directory***.

В модели стандартного сохранения зон обновления ***DNS*** выполняются на основе модели с единственным главным сервером. В такой модели единственный удостоверяющий ***DNS***-сервер зоны обозначается как основной источник для зоны. Это сервер содержит главную копию зоны в файле на локальном диске. В этой модели основной сервер зоны представляет

единственную фиксированную точку отказа. Если этот сервер недоступен, запросы на обновление зоны от ***DNS***-клиентов не обрабатываются. При сохранении зон, интегрированных в службу каталогов, динамические обновления ***DNS***выполняются с использованием модели с несколькими главными серверами. В этой модели любой удостоверяющий ***DNS***-сервер, например, контроллер домена, выполняющий службу ***DNS***-сервер, обозначается как основной источник для зоны. Поскольку главная копия зоны поддерживается в базе данных ***Active Directory***, которая полностью реплицируется на все контроллеры домена, зона может обновляться любыми ***DNS***-серверами, выполняющимися на любом контроллере домена.

При использовании модели ***Active Directory*** с несколькими главными серверами любой из основных серверов для зоны, интегрированной в каталоги, может обрабатывать запросы от ***DNS***-клиентов на обновление зоны, пока контроллер домена является доступным по сети. Кроме того, при использовании зон, интегрированных в службу каталогов, можно с помощью списков управления доступом защитить объект-контейнер **dnsZone** в дереве каталогов. Это средство обеспечивает дифференцированный доступ к зоне или к конкретной записи ресурса в зоне. Например, список управления доступом для записи ресурса в зоне можно ограничить так, чтобы разрешить динамические обновления только указанному компьютеру клиента или группе безопасности, например, группе администраторов домена. Это средство безопасности недоступно для стандартных основных зон. Необходимо отметить, что при преобразовании зоны к типу интегрированной в службу каталогов настройка по умолчанию для обновлений зоны изменяется и разрешаются только безопасные обновления. Кроме того, при использовании списков управления доступом на объектах ***Active Directory***, относящихся к ***DNS*** , списки управления доступом могут применяться только к службе ***DNS***-клиент.

• Репликация и синхронизация зон с новыми контроллерами домена выполняется автоматически при каждом добавлении нового контроллера в домен ***Active Directory***.

Хотя службу ***DNS*** можно выборочно удалять с контроллеров домена, зоны, интегрированные в службу каталогов, всегда сохраняются на каждом контроллере домена. В результате сохранение и управление зонами не является дополнительным ресурсом. Кроме того, способы синхронизации информации, сохраняемой в службе каталогов, обеспечивают повышение быстродействия по сравнению со стандартными способами сохранения обновлений зон, которые могут потенциально потребовать передачи зоны целиком.

• За счет сохранения баз данных зон ***DNS*** в ***Active Directory*** имеется возможность рационализировать репликацию баз данных в сети.

Когда пространство имен ***DNS*** и домены ***Active Directory*** сохраняются и реплицируются независимо, необходимо обеспечить планирование и администрирование каждого из них в отдельности. Например, при одновременном использовании стандартного сохранения зон ***DNS*** и службы каталогов ***Active Directory*** необходимо обеспечить структуру, реализацию,

тестирование и управление для двух различных топологий репликации баз данных. Одна топология требуется для репликации данных из каталогов между контроллерами домена, а другая топология может потребоваться для репликации баз данных зон между ***DNS***-серверами.

Это приведет к дополнительным трудност+ям при планировании и разработке структуры сети с учетом ее естественного роста. За счет интеграции сохранения информации ***DNS*** появляется возможность унифицировать вопросы управления и репликации для ***DNS*** и ***Active Directory***, объединяя их в единое административное целое.

• Репликация каталогов выполняется быстрее и эффективнее, чем стандартная репликация ***DNS***.

Поскольку репликация ***Active Directory*** выполняется на уровне отдельных свойств, распространяются только необходимые изменения. При этом для зон, интегрированных в службу каталогов, используется и отправляется меньший объем данных.

Выполнение работы

Задание 1. Установка сервера DNS

1. Запустите виртуальную машину ВМ **VM-2**.
2. Подключите к виртуальной машине образ установочного диска ***win2003.iso***.
3. Откройте диалоговое окно **Управление данным сервером (*Пуск/Администрирование/Управление Данным Сервером*)**.
4. Активизируйте установку сервера имен:
   - запустите мастер добавления ролей сервера, кнопкой ***Добавить или удалить роль*** 

;
   - ознакомьтесь с информацией мастера и продолжите установку кнопкой ***Далее***;
   - укажите тип установки Особая конфигурация и продолжите установку кнопкой ***Далее***.
   - выберите в списке доступных ролей сервера пункт ***DNS***-сервер. Нажмите ***Далее***.
   - Ознакомьтесь с сводкой выбранных параметров и продолжите установку кнопкой ***Далее***.

*После завершения установки сервера имен, автоматически запуститься **Мастер настройки DNS-сервера**.*

5. Выполните первоначальную настройку ***DNS***-сервера с помощью мастера:
   - ознакомьтесь с информацией мастера (***Далее***);
   - ознакомьтесь с предлагаемыми вариантами настройки сервера;
   - выберите создание зоны прямого просмотра для небольших сетей, соответствующей радиокнопкой (***Далее***);

- укажите ваш ***DNS***-сервер в качестве ***DNS***-сервера, который будет обслуживать зону прямого просмотра, радиокнопкой *Управление зоной выполняется этим сервером*. Продолжите установку кнопкой ***Далее***;

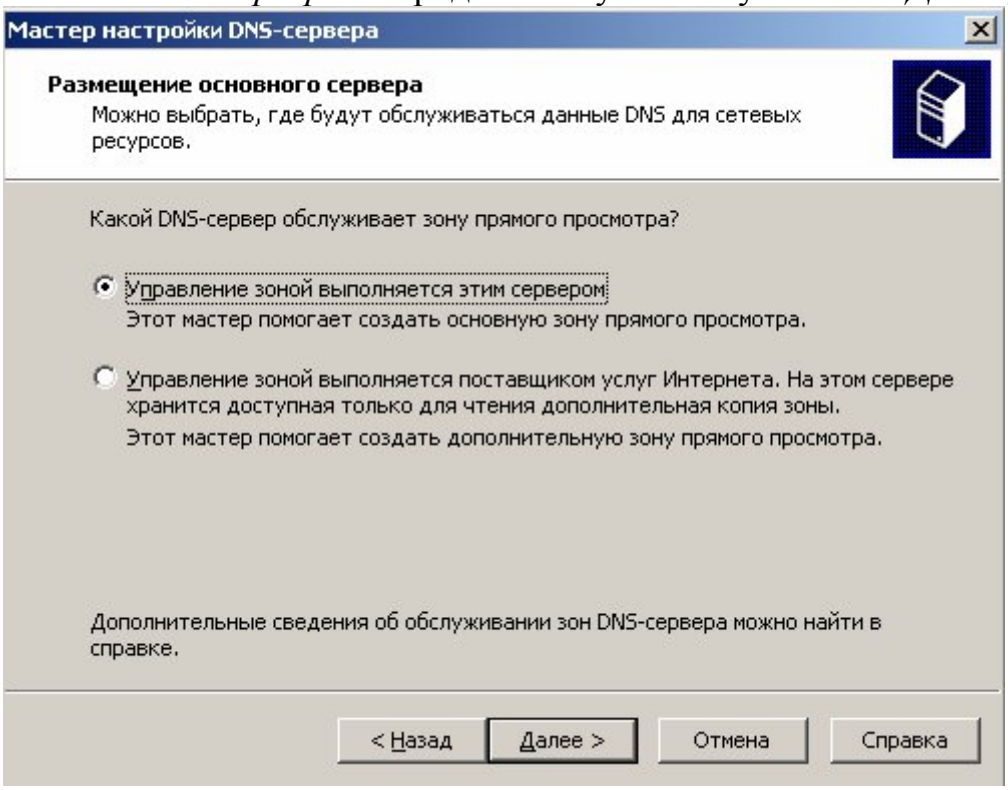

Рисунок 4. Размещение основного сервера

- задайте имя зоны, например **example.edu.ru** и продолжите установку кнопкой ***Далее***.
- введите в поле **Создать новый файл** имя файла (например *example.edu.ru.dns*)в котором будет храниться конфигурация зоны. Продолжите установку кнопкой ***Далее***;
- запретите динамическое обновление соответствующей радиокнопкой и продолжите настройку кнопкой ***Далее***;
- откажитесь от пересылки запросов на другие ***DNS***-сервера, выбрав радиокнопку *Нет, не пересылать запросы* (***Далее***);
- ознакомьтесь с информацией о недоступности корневых сертификатов и щелкните ***ОК***;
- завершите первоначальную настройку ***DNS***-сервера кнопкой ***Готово***.

Задание 2. Настройка сервера DNS.

1. Переключитесь в диалоговое окно ***Управления данным сервером***.
2. Перейдите в управление ***DNS***-сервером, кнопкой ***Управление этим DNS-сервером***. *Появится окно консоли администрирования, с открытой оснасткой управления* ***DNS****-сервером*

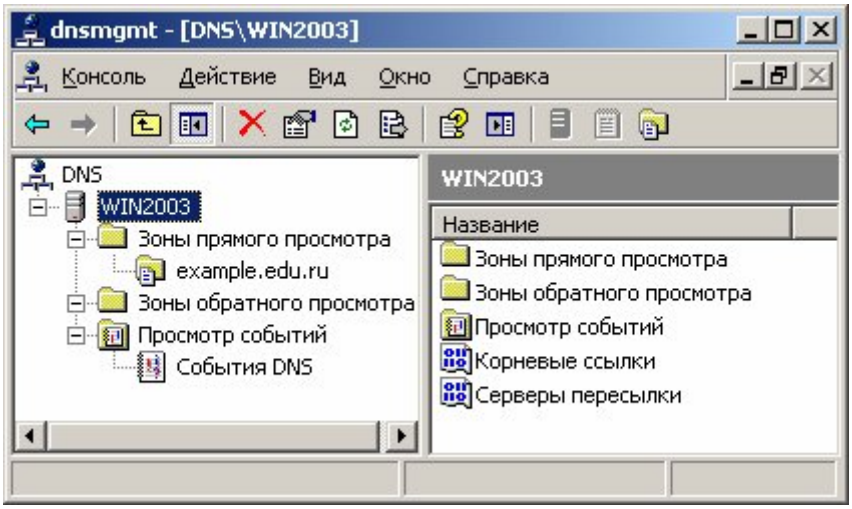

Рисунок 5. Создание зоны прямого просмотра.

3. Настройте зону прямого просмотра:

- откройте диалоговое окно свойств созданной ранее зоны **example.edu.ru (*контекстное меню/Свойства*)**
- настройте очистку и обновление содержимого ***DNS***-сервера:
  - откройте окно очистки, кнопкой ***Очистка***;
  - установите флажок *Удалять устаревшие записи ресурсов*;
  - установите **интервал блокирования** - *1 день*;
  - установите **интервал обновления** - *7 дней*;
  - подтвердите изменения кнопкой ***ОК***.
- установите **срок жизни (TTL) записи** – *2 часа*:
  - перейдите на вкладку **Начальная запись зоны (SOA)**;
  - введите в поле **Срок жизни (TTL) записи** – *0: 2: 0: 0*;
  - установите **желаемые интервалы для обновления и повтора** - *не менее 1 и не более 15 минут*.

Завершите настройку кнопкой ***ОК***.

4. Создайте запись в ***DNS***-сервере соответствующую физическому компьютеру:

- откройте диалоговое окно **добавления новых узлов (*контекстное меню example.edu.ru/Создать узел (A)*)**;
- введите в поле **Имя** - *<имя_физического_компьютера>*;
- введите в поле **IP-адрес** - *192.168.1.1*;
- завершите добавление кнопкой ***Добавить***.

5. Создайте новую основную зону обратного просмотра:

- откройте **мастер создания новых зон (*контекстное меню Зоны обратного просмотра/Создать новую зону*)**;
- ознакомьтесь с информацией мастера и щелкните ***Далее***;
- укажите **тип создаваемой зоны** - *Основная зона* (***Далее***);
- укажите **код сети** – *192.168.1* (***Далее***);

Поскольку IP-адреса создаваемой сети к сети класса С, то в IP-адресах сети будет меняться только последний разряд адреса.

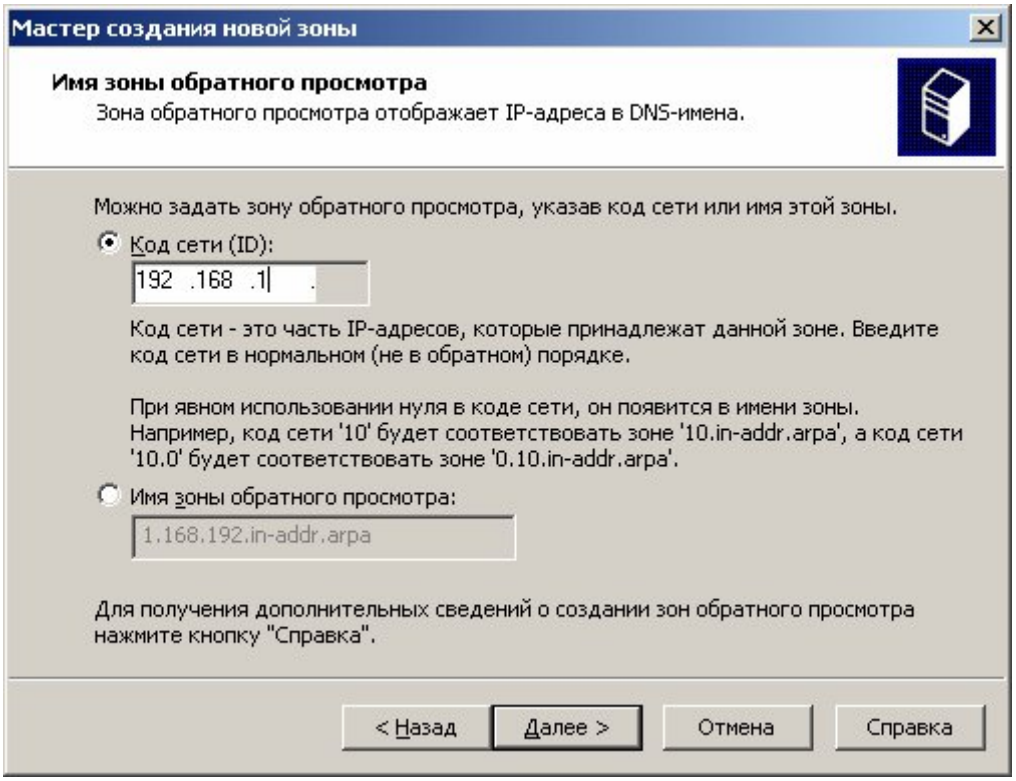

Рисунок 6. Задание кода сети

- укажите имя файла для зоны по умолчанию и продолжите установку кнопкой ***Далее***.
- установите запрет динамических обновлений (***Далее***);
- завершите создание зоны кнопкой ***Готово***.

6. Протестируйте работу ***DNS***-сервера:

- откройте диалоговое окно свойств ***DNS***-сервера (***контекстное меню Wind2003/Свойства***);
- перейдите на вкладку **Наблюдение**;
- установите флажок *Простой запрос к этому DNS-серверу*;
- активируйте тестирование кнопкой ***Тест***; *Результат отобразиться в поле* ***Результаты теста***.
- создайте и сохраните в своей папке снимок экрана с результатами теста;
- закройте диалоговое окно свойств кнопкой ***ОК***.

7. Выключите ВМ.

Лабораторная работа 2. Настройка параметров безопасности домена

Цель: научиться устанавливать и просматривать Active Directory, научится подключать компьютеры к домену.

Средства для выполнения работы:

- аппаратные: компьютер;
- программные: ОС Windows 2003 server.

Теоретические сведения

Словосочетание *"информационная безопасность"* в разных контекстах может иметь различный смысл. В **Доктрине информационной безопасности Российской Федерации** термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В **Законе РФ "Об участии в международном информационном обмене"** информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под ***информационной безопасностью*** будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Комплекс работ по внедрению политики информационной безопасности можно разделить на 3 этапа

На первом этапе определяются общие подходы к политике ИБ, определяются группы ИБ и общее описание разрешений.

На втором этапе осуществляется документирование политики ИБ: составление правил и инструкций для работников организации.

На третьем этапе осуществляется реализация (внедрение) политики ИБ как программными, так и аппаратными средствами.

Следует разработать ряд правил, которые помогут регламентировать работу всех пользователей в сети (как привилегированных так и не привилегированных). В частности следует разработать:

- правила административного обслуживания;
- перечень прав и обязанностей пользователей;
- правила для администраторов;
- правила создания «гостевых» учетных записей.

Разработка таких правил позволит получить ряд преимуществ:

- рутинные задачи всегда выполняются одинаково;
- уменьшение вероятности появления ошибок;
- работа по инструкциям выполняется гораздо быстрее.

Помимо разработки ряда правил для пользователей следует предусмотреть (разработать) стандартные методики:

- подключения и конфигурирования и модернизации компьютеров;
- инсталляции и деинсталляции программного обеспечения;
- резервного копирования данных;
- назначения адресов;
- и т.д.

Например, считается, что управление адресами и именами компьютеров, идентификаторами пользователей и групп должно осуществляться единообразно.

Правила для пользователей

Во многих организациях существуют специально разработанные правила пользователей, только после подписания, которых пользователь получает доступ к сети организации.

В правилах для пользователя необходимо регламентировать такие вопросы:

- использование учетных записей совместно с друзьями и родственниками;
- использование программ дешифровки паролей;
- нарушение нормального процесса обслуживания;
- использование чужих учетных записей;
- использование файлов, чужих учетных записей;
- использование системных ресурсов;
- копирование защищенных авторскими правами материалов;
- возможная незаконная деятельность (мошенничество, клевета и др.).
- вовлечение в деятельность, которая является незаконной.

Правила для администраторов

В правилах для администраторов должны быть сформулированы руководящие принципы использования предоставленных привелегий и соблюдения секретности пользовательских данных. Следует особо отметить использование учетных записей строго индивидуально.

Правила и методики для экстренных случаев

Следует заблаговременно предусмотреть действия при различных нештатных ситуациях. Например, для аварийных ситуаций следует указать лиц с их телефонами, которых надо предупредить в первую очередь. При выходе из строя программного обеспечения можно указать серийные номера для их самостоятельной переустановки или контактную информацию поставщика программного обеспечения.

Безопасность в домене под управлением Windows

Преимущества использования групповой политики:

- При интеграции со службой ***Active Directory*** позволяет как централизованно, так и децентрализовано управлять параметрами безопасности и настройками пользователей.
- Обладает гибкостью и масштабируемостью. Может быть применена в широком наборе конфигураций системы.

• Предоставляет администратору единый инструмент управления с простым и понятным интерфейсом – **Групповая политика**.

• Обладает высокой степенью надежности и безопасности.

Политика безопасности в сети на основе **Windows** храняться в двух типах объектов:

• локальный объект групповой политики;

• объект групповой политики домена.

Для работы с объектами групповой политики используется оснастка **Групповая политика**, которая может запускаться как для локального компьютера, так и для удаленного.

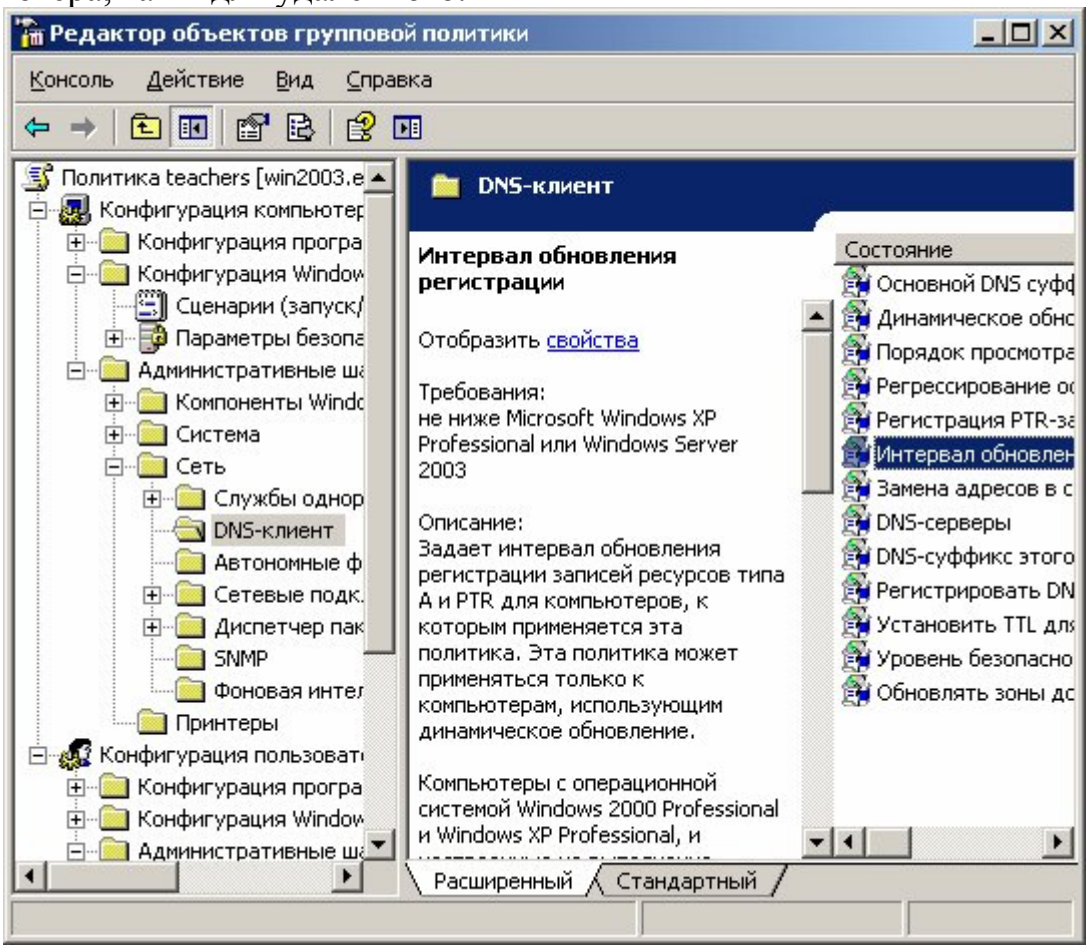

Рисунок 1. Редактор объектов групповой политики.

В структуре объекта групповой политики выделяется 2 раздела (узла):

• *Узел конфигурации компьютера.* Содержит параметры всех политик, определяющих работу компьютера. Они регулируют параметры функционирования операционной системы, определяют права пользователей в системе.

• *Узел конфигурации пользователя.* Содержит параметры всех политик, определяющих работу пользователя на компьютере. Они регулируют вид рабочего стола и конфигурацию рабочей среды, управляют пользовательскими сценариями входа и выхода.

Каждый из перечисленных выше узлов содержит:

• *Административные шаблоны.* Здесь находится групповая политика, определяющая параметры реестра, задающие работу в и внешний вид рабочего стола, компоненты операционной системы и приложений.

• *Параметры безопасности.* Служит для настройки параметров системы безопасности компьютеров: политик аудита и блокировки учетных записей, права пользователя и т.п.

• *Установка программ.* Служит для централизованного управления программным обеспечением организации. С его помощью моэно задать различные режимы установки новых программ на компьютеры пользователей.

• *Сценарии.* Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы.

• *Перенаправление папок.* Позволяет перенаправлять обращение к специальным папкам в сеть.

Выполнение работы

Задание 1. Создайте документы, описывающие политику информационной безопасности для ВУЗа, и сохраните их в личной папке.

• правила административного обслуживания;

• перечень прав и обязанностей пользователей;

• правила для администраторов;

• правила создания «гостевых» учетных записей.

Задание 2. Создание и редактирование групповой политики.

1. Откройте диалоговое окно оснастки **Пользователи и компьютеры (*Пуск/Администрирование/Active Direcory – Пользователи и компьютеры*)**.

2. Выполните редактирование политики безопасности домена, созданную автоматически:

- откройте диалоговое окно свойств домена **example.edu.ru (контекстное меню/Свойства)**;
- перейдите на вкладку **Групповая политика**;

В списке будет расположена политика домена по умолчанию Default Domain Policy.

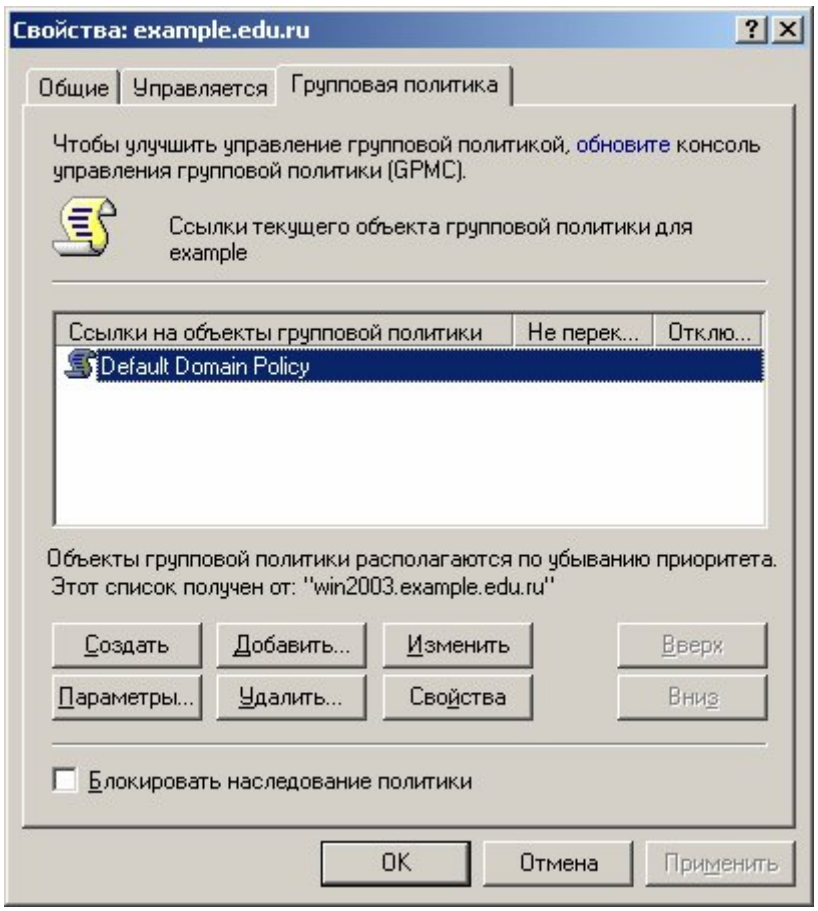

Рисунок 2. Свойства домена.

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики **Default Domain Policy** (двойной щелчок по политике);

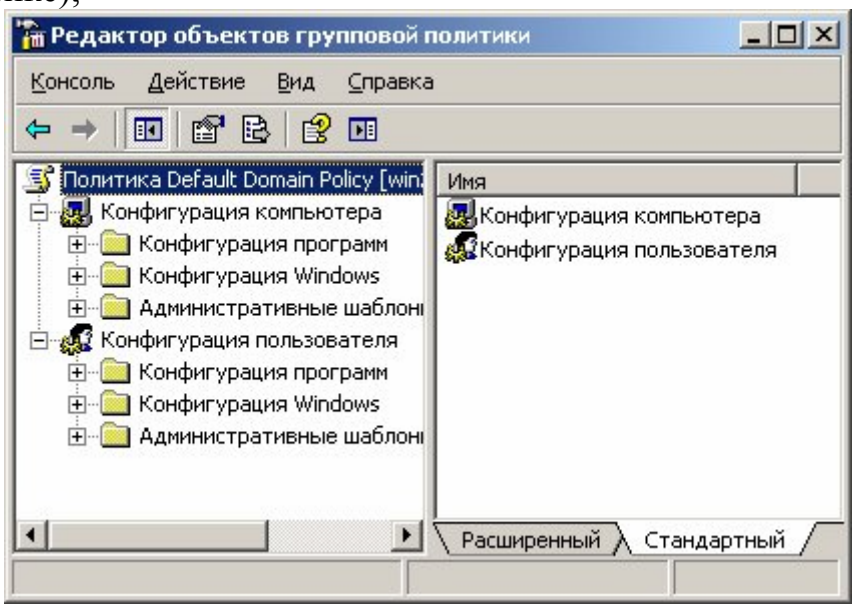

Рисунок 3. Редактор объектов групповой политики.

- внесите в изменения в политику паролей:
  - перейдите в раздел **Политика паролей (*Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/Политики паролей*)**;

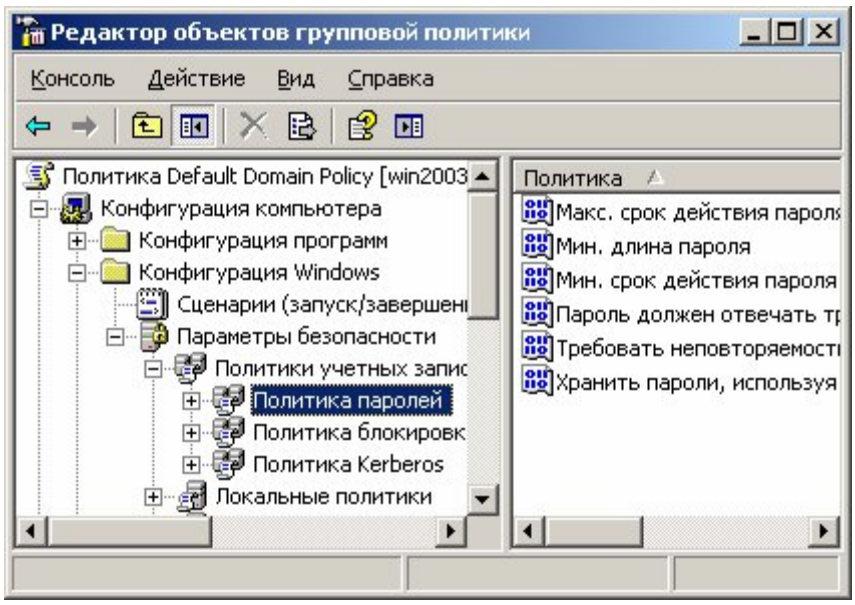

Рисунок 4. Политика паролей.

- установите **минимальную длину пароля**: откройте окно изменения параметров пароля (двойной щелчок по надписи **Мин. длинна пароля**) и введите в поле **Длина пароля не менее**– *5 (**ОК**)*;
- отключите **соответствие пароля требованиям сложности**:
- откройте диалоговое окно свойств требования сложности (двойной щелок по надписи **Пароль должен отвечать требованиям сложности**);
- установите радиокнопку *Отключить*;
- подтвердите изменения кнопкой ***ОК***;
- отключите **возможность использования экранных заставок**:
- перейдите в раздел **Экран (*Конфигурация пользователя/Административные шаблоны/Экран*)**;
- откройте диалоговое окно свойств **Использовать экранные заставки** и выберите *Отключен*;
- подтвердите изменения кнопкой ***ОК***.

- закройте **Редактор объектов групповой политики (*Консоль/Выход*)**;
- закройте диалоговое окно свойств домена кнопкой ***ОК***.

3. Создайте новую политику для учителей:

- откройте диалоговое окно свойств домена **example.edu.ru (*контекстное меню/Свойства*)** и перейдите на вкладку **Групповая политика**;
- активизируйте создание новой политики кнопкой ***Создать***;
- введите название политики - *Teachers*;
- самостоятельно измените созданную политику, отключив пользователям возможность менять фон рабочего стола.

4. Закройте редактор объектов групповой политики.

Задание 3. Создание групп и учетных записей пользователей.

1. Откройте оснастку **Пользователи и компьютеры**.
2. Создайте новую учетную запись пользователя в контейнере **Students**:

- откройте диалоговое окно **Новый объект – Пользователь**, кнопкой ***Создание нового пользователя в текущем контейнере*** ;
- введите данные о пользователе:
  - **Полное имя пользователя** – *Просто Пользователь*;
  - **Имя входа пользователя (логин)** – *JustUser*;
  - Подтвердите введенные данные кнопкой ***Далее***.

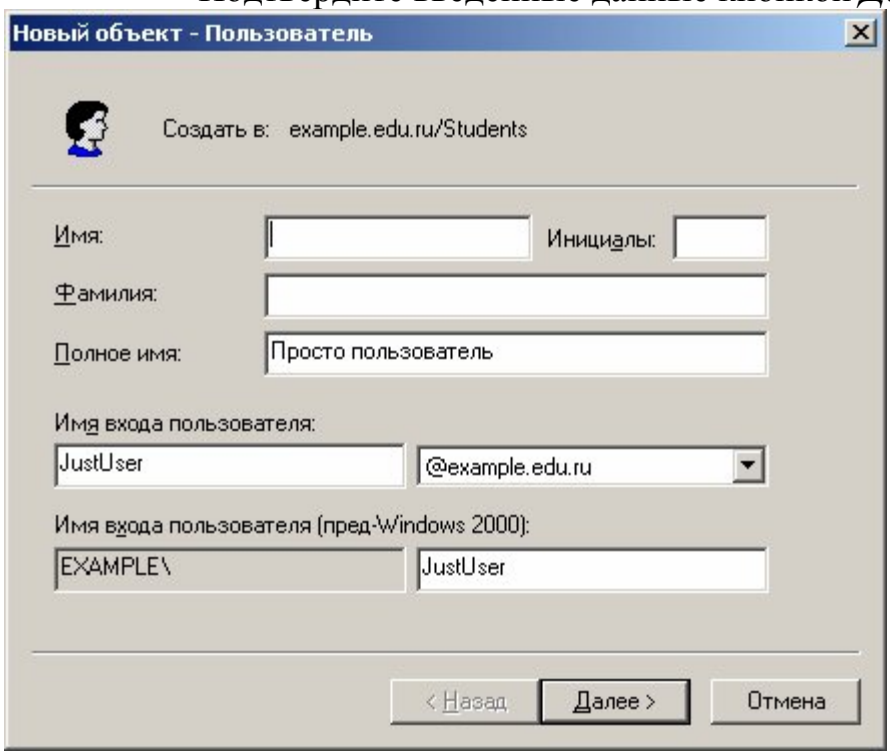

Рисунок 5. Ввод данных нового пользователя.

- установите пароль для пользователя:
  - введите в поле **Пароль** – *User1234*;
  - введите в поле **Подтверждение** – *User1234*;
  - установите флажок *Срок действия пароля не ограничен*;
  - завершите ввод пароля кнопкой ***Далее***.

В правой области отобразиться запись, соответствующая созданному пользователю.

3. Введите более полную информацию о пользователе:
   - откройте диалоговое окно свойств пользователя (двойной щелчок по надписи **Просто пользователь**);
   - введите в поле **Описание** – *это тестовый пользователь*;
   - введите в поле **Комната** - номер кабинета в котором проходит занятие - *316*;
   - введите в поле **Телефон** – <номер своего мобильного телефона>;
   - укажите адресные данные на вкладке **Адрес**;
   - укажите несколько дополнительных телефонов пользователя на вкладке **Телефоны**;
   - завершите изменение данных пользователя кнопкой ***ОК***.
4. Создайте группу **group1** в контейнере **Students**:

- откройте диалоговое окно создания групп (***контекстное меню/Создать/Группа***);
- введите **имя группы – *group1*;**
- **завершите создание группы кнопкой *ОК*.**

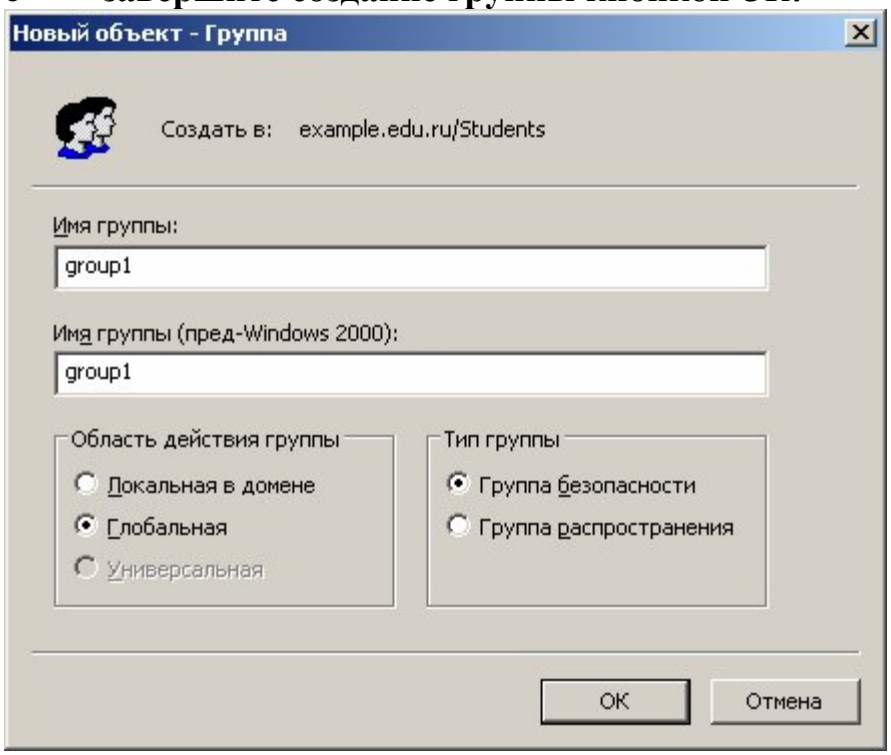

Рисунок 6. Создание группы.

5. Задайте дополнительную информацию для группы group1:

- **откройте диалоговое окно свойств группы (*двойной щелчок по надписи group1*);**
- **введите в поле Описание – *Это тестовая группа*;**
- **завершите изменение данных группы кнопкой *ОК*.**

6. Включите созданного ранее пользователя *Просто пользователь (JustUser)* в группу group1:

- **откройте диалоговое окно свойств пользователя (*двойной щелчок по записи пользователя*);**
- **перейдите на вкладку Член групп;**
- **откройте диалоговое окно выбора группы кнопкой *Добавить*;**
- **введите название группы – *group1*;**
- **завершите добавления пользователя в группу кнопкой *ОК*.**
- **закройте диалоговое окно свойств пользователя кнопкой *ОК*.**

7. **Выполните выход из системы с повторным входом для активации изменений в политике безопасности.** ***Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.***

8. Измените пароль созданного ранее пользователя:

- **активизируйте раздел Students;**
- **задайте новый, более простой пароль пользователю Просто пользователь:**

- **откройте диалоговое окно задания пароль (*контекстное меню/Смена пароля*);**
- **введите в поле Пароль – *123*;**
- **введите в пол Подтверждение пароля – *123*;**

Обратите внимание что сообщений по слишком простом пароле не было.

-

9. Исключите созданного ранее пользователя из группы group1:

- **откройте диалоговое окно свойств группы;**
- **перейдите на вкладку Члены группы;**
- **выделите в списке удаляемого пользователя и щелкните по кнопке *Удалить*;**
- **подтвердите удаление кнопкой *Да*;**
- **закройте диалоговое окно свойств группы кнопкой *ОК*.**

10. Включите созданного ранее пользователя в администраторы домена:

- **откройте диалоговое окно свойств пользователя Просто пользователь;**
- **перейдите на вкладку Член групп и щелкните *Добавить*;**
- **введите в поле *Администраторы домена*;**
- **завершите добавление в группу кнопкой *ОК*;**
- **закройте окно свойств пользователя кнопкой *ОК*.**

11. **Закройте оснастку Пользователи и компьютеры.**

Лабораторная работа 3. Работа с Active Directory

Цель: научиться устанавливать и просматривать Active Directory, научится подключать компьютеры к домену.

Средства для выполнения работы:

• аппаратные: компьютер с установленной ОС Windows XP.

• программные: приложение ВМ: VirtualBox; виртуальные машины: VM-1, VM-2.

Теоретические сведения

Active Directory является **LDAP** (***Lightweight Directory Access Protocol*** — «облегчённый протокол доступа к каталогам»)-совместимой реализацией **службы каталогов** (это средство иерархического представления ресурсов, принадлежащих некоторой отдельно взятой организации, и информации об этих ресурсах) корпорации **Microsoft** для операционных систем семейства **Windows NT**. *Active Directory* позволяет администраторам использовать глобальные политики, развёртывать программы на множестве компьютеров (через глобальные политики или посредством **Microsoft Systems Management Server 2003**) и устанавливать важные обновления на всех компьютерах в сети (с использованием **Windows Server Update Services (WSUS); Software Update Services (SUS)** ранее). *Active Directory* хранит данные и настройки среды в централизованной базе данных. Сети *Active Directory* могут быть различного размера: от нескольких сотен до нескольких миллионов объектов.

Помимо обычных для служб каталогов задач, *Active Directory* способна удовлетворить широкий спектр потребностей по обработке имен, обслуживанию запросов, регистрации, администрированию и устранению конфликтов. В *Active Directory* используется тесно увязанный набор **API** и протоколов, так что она может работать с несколькими пространствами имен, собирать и предоставлять информацию о каталогах и ресурсах, находящихся в удаленных филиалах и под управлением разных ОС. *Active Directory* имеет следующие возможности и характеристики:

• Поддержка открытых стандартов для облегчения межплатформных операций с каталогами, в т. ч. доменной системы имен ***DNS*** и стандартных протоколов, таких как **LDAP** (***Lightweight Directory Access Protocol*** — «облегчённый протокол доступа к каталогам»).

• Поддержка стандартных форматов имен для простоты миграции и эксплуатации.

• Богатый набор **API**, которые могут использоваться как для командных сценариев, так и в программах на **C/C++**.

• Простой и интуитивно понятный процесс администрирования благодаря несложной иерархической доменной структуре и использованию технологии «перетащить и оставить».

• Возможность расширения набора объектов в каталогах, за счет гибкой логической схемы.

• Быстрый поиск по глобальному каталогу.

• Быстрое и удобное обновление информации посредством многоуровневой (*multimaster*) репликации данных.

• Совместимость с предыдущими версиями ОС **Windows NT**.

• Взаимодействие с сетями **NetWare**.

Active Directory позволяет управлять с одного рабочего места всеми заявленными ресурсами (файлами, периферийными устройствами, базами данных, подключениями к серверам, доступом к Web, пользователями, другими объектами, сервисами и т. д.). В качестве идентификационной службы в ней используется доменная система имен (***DNS***), применяемая в Интернете, объекты в доменах строятся в иерархию организационных единиц (***OE***), а домены могут быть объединены в древовидную структуру. Администрирование становится еще проще, так как в *Active Directory* отсутствует понятие главного контроллера доменов (***ГКД***) и резервного контроллера доменов (***РКД***). В *Active Directory* существуют только контроллеры домена (***КД***), и все они равны между собой. Администратор может сделать изменения на любом ***КД***, и эти изменения будут скопированы на всех остальных ***КД***.

Active Directory отделяет логическую структуру иерархии доменов **Windows 2003** от физической структуры сети. *Объекты:* ресурсы хранятся в виде объектов. Схема *Active Directory*:

• Домены: базовая организационная структура.

• Деревья: несколько доменов объединяются в иерархическую структуру.

• Леса: группа из нескольких деревьев домена.

Организационные единицы: позволяют делить домен на зоны и делегировать на них права.

Логическая структура *Active Directory* не базируется на физическом местонахождении серверов или сетевых соединениях в пределах домена. Это позволяет структурировать домены, отталкиваясь не от требований физической сети, а от административных и организационных требований.

Объекты хранятся в *Active Directory* в виде иерархической структуры контейнеров и подконтейнеров, упрощающей поиск, доступ и управление, она во многом похожа на файловую систему**Windows** с файлами в папками.

Классы объектов. Объект на самом деле представляет собой просто набор атрибутов. Например, объект пользователя (*user object*) состоит из таких атрибутов, как имя, пароль, телефонный номер, сведения о членстве в группах и т. д. Атрибуты, образующие объект, определяются классом объекта.

Классы и атрибуты, определяемые ими, собирательно называются *Active Directory Schema* — в терминологии баз данных схема (*schema*) — это структура таблиц и полей, а также их взаимосвязи.*Active Directory Schema* можно считать набором данных (классов объектов), определяющим то, как организована и хранится реальная информация (атрибуты объекта) в каталоге.

Active Directory — не первая служба каталогов. В современных сетях используется несколько служб каталогов и стандартов. Вот лишь некоторые из них:

• **X.500** и **Directory Access Protocol (DAP). X.500** — спецификация **Internet Standards Organization (ISO)**, определяющая, как должны быть структурированы глобальные каталоги. **X.500** также описывает применение **DAP** для обеспечения взаимодействия между клиентами и серверами каталогов;

• **Lightweight Directory Access Protocol (LDAP). LDAP** была разработана в ответ на критические замечания по **DAP**, которая оказалась слишком сложной для применения в большинстве случаев.**LDAP** быстро стала стандартным протоколом каталогов в Интернете.

• **Novell Directory Services (NDS)**. Служба каталогов для сетей **Novell NetWare**, совместимая со стандартом **X.500**.

• **Active Directory**. Составная часть сетей под управлением **Windows Server 2000** или **Windows Server 2003**. Соответствует стандарту **LDAP**.

Выполнение работы

Задание 1. Установите Active Directory.

1. Подготовьте виртуальную машину **VM-2** к установке службы каталогов:
   - подключите к ВМ образ установочного диска ***win2003-1.iso***;
2. Откройте диалоговое окно **Управление данным сервером (*Пуск/Администрирование/Управление Данным Сервером*)**.
3. Проверьте наличие установленного сервера доменных имен (***DNS***). *Установка службы каталогов невозможна без **DNS**.*
4. Активизируйте добавление новых ролей для сервера (***Добавить или удалить роль***).
5. Выберите пункт **Контроллер домена (Active Directory)** . Перейдите к следующему шагу кнопкой ***Далее***.
6. Ознакомьтесь с информацией об устанавливаемых компонентах и щелкните ***Далее***.
7. Ознакомьтесь с информацией **Мастера установки Active Directory** и щелкните ***Далее***.
8. Ознакомьтесь с информаций о совместимости с операционной системой и щелкните ***Далее***.
9. Укажите **вариант созданий контроллера домена** - *Контроллер домена в новом домене* и щелкните ***Далее***.
10. Укажите **тип создаваемого домена** - *Новый домен в новом лесу* и щелкните ***Далее***.
11. Введите **полное DNS-имя создаваемого домена** - *example.edu.ru* и щелкните ***Далее***.
12. Введите **NetBIOS-имя домена** - *EXAMPLE* и щелкните ***Далее***. *Обычно оно уже указанно по умолчанию, исходя из того, какое **DNS**-имя было дано создаваемому домену. Например, при создании домена с именем **example.edu.ru**, по умолчанию **NETBIOS-имя**будет **EXAMPLE**.*
13. Укажите место хранения баз данных и журналов *Active Directory*:
    - введите в поле **Папка расположения Баз - *C:\WINDOWS\NTDS\BASE***;

- введите в поле **Папка расположения журнала - *C:\WINDOWS\JOURNAL***;
- подтвердите изменения кнопкой ***Далее***.

14. Ознакомьтесь с информацией об общей папке и щелкните ***Далее***. *Если ваш **DNS**-сервер настроен неправильно, вы получите сообщение об ошибке и возможных путях её устранения (выберите **Проблема будет решена позже**)*.

15. Установите разрешения для объектов службы каталогов - *Разрешения, совместимые только с Windows 2000 или Windows Server 2003* и щелкните ***Далее***.

16. Укажите пароль, для учётной записи администратора режима восстановления:
- введите в поле **Пароль режима восстановления** – *123456*;
- введите в поле **Подтверждение** – *123456*;
- подтвердите изменения кнопкой ***Далее***.

17. Ознакомьтесь с сводной информацией об установке службы каталогов и запустите ее установку кнопкой ***Далее***.

18. Завершите работу мастера кнопкой ***Готово***.

19. Перезагрузите виртуальную машину кнопкой ***Перезагрузить сейчас***.

20. Войдите в систему после перезагрузки и завершите установку службы каталогов кнопкой ***Готово***.

Задание 2. Работас Active Directory Manager

1. Откройте диалоговое окно **Пользователи и компьютеры (*Пуск/Администрирование/Active Directory – пользователи и компьютеры*)**.

2. Ознакомьтесь с структурой созданного ранее домена:
- разверните узел **example.edu.ru**;

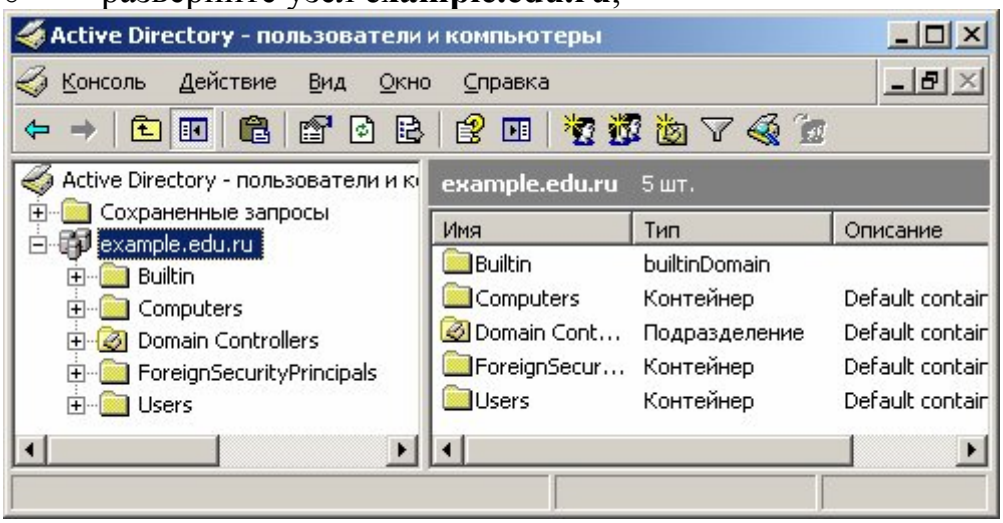

Рисунок 1. Пользователи и компьютеры домена.

- просмотрите стандартных пользователей домена (**Builtin**);
- просмотрите контроллеры домена (**Domain Controllers**).

3. Создайте новый каталог (подразделение/контейнер) в корне сервера:
- активизируйте узел **example.edu.ru**;
- щелкните по кнопке ***Создание нового подразделения в текущем контейнере*** на панели инструментов;

- в появившемся диалоговом окне введите **имя создаваемого подразделения** - *Students* (***OK***);

Будет создан новый контейнер для подразделения и выделение автоматически переместиться на него.

4. Создайте новую учетную запись пользователя в контейнере **Students**:

- откройте диалоговое окно **Новый объект – Пользователь**, кнопкой ***Создание нового пользователя в текущем контейнере*** ;
- введите данные о пользователе:
  - **Полное имя пользователя** – *Просто Пользователь*;
  - **Имя входа пользователя (логин)** – *JustUser*;
  - Подтвердите введенные данные кнопкой ***Далее***.

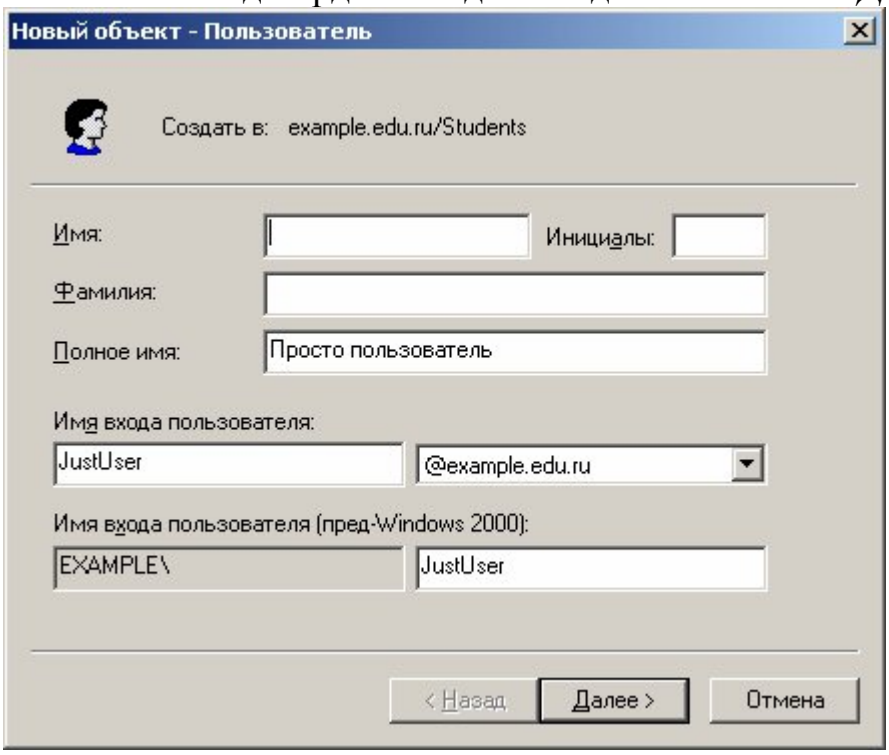

Рисунок 2. Ввод данных нового пользователя.

- установите пароль для пользователя:
  - введите в поле **Пароль** – *User1234*;
  - введите в поле **Подтверждение** – *User1234*;
  - установите флажок *Срок действия пароля не ограничен*;
  - завершите ввод пароля кнопкой ***Далее***.

В правой области отобразиться запись, соответствующая созданному пользователю.

5. Введите более полную информацию о пользователе:

- откройте диалоговое окно **свойств пользователя** (двойной щелчок по надписи ***Просто пользователь*)**;
- введите в поле **Описание** – *это тестовый пользователь*;
- введите в поле **Комната** - *316* (номер кабинета, в котором проходит занятие);
- введите в поле **Телефон** – *<номер_телефона>*;

- укажите *адресные данные* на вкладке **Адрес**;
- укажите несколько дополнительных телефонов пользователя на вкладке **Телефоны**;
- завершите изменение данных пользователя кнопкой ***ОК***.

6. Создайте группу **group1** в контейнере **Students**:
   - откройте диалоговое окно **создания групп (*контекстное меню/Создать/Группа*)**;
   - введите **имя группы** – *group1*;
   - завершите создание группы кнопкой ***ОК***.

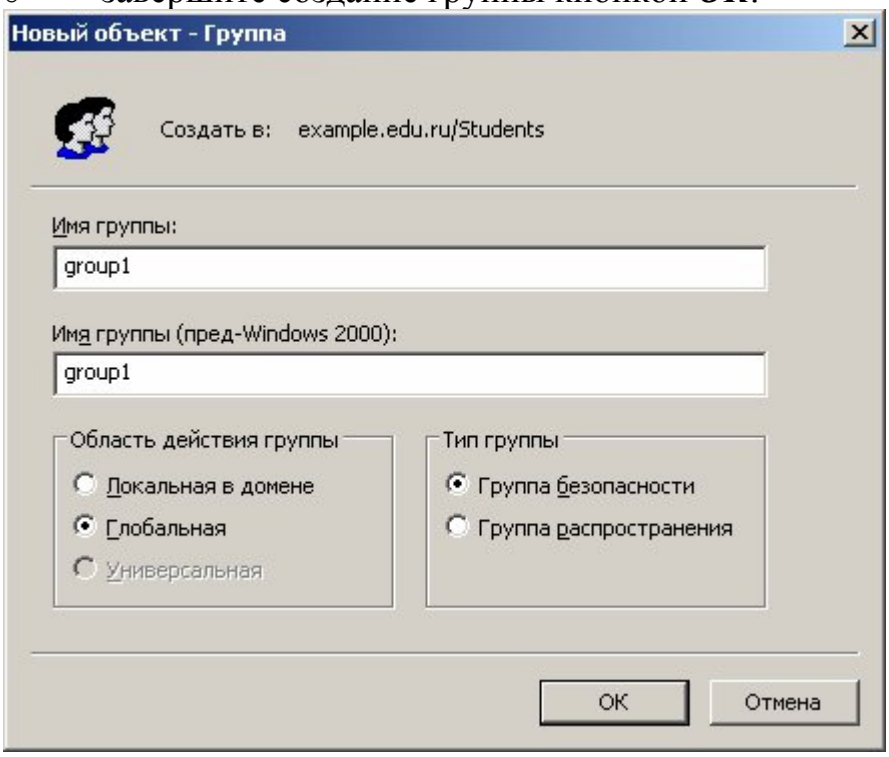

Рисунок 3. Создание группы.

7. Задайте дополнительную информацию для группы **group1**:
   - откройте диалоговое окно **свойств группы** (двойной щелчок по надписи **group1**);
   - введите в поле **Описание** – *Это тестовая группа*;
   - завершите изменение данных группы кнопкой ***ОК***.

8. Включите созданного ранее пользователя **Просто пользователь (*JustUser*)** в группу **group1**:
   - откройте диалоговое окно **свойств пользователя** (двойной щелчок по записи пользователя);
   - перейдите на вкладку **Член групп**;
   - откройте диалоговое окно выбора группы кнопкой ***Добавить***;
   - введите **название группы** – *group1*;
   - завершите добавления пользователя в группу кнопкой ***ОК***.
   - закройте диалоговое окно свойств пользователя кнопкой ***ОК***.

9. Выполните редактирование политики безопасности домена, созданную автоматически:

- откройте диалоговое окно свойств домена **example.edu.ru (*контекстное меню/Свойства*)**;
- перейдите на вкладку **Групповая политика**:

*В списке будет расположена политика домена по умолчанию **Default Domain Policy**.*

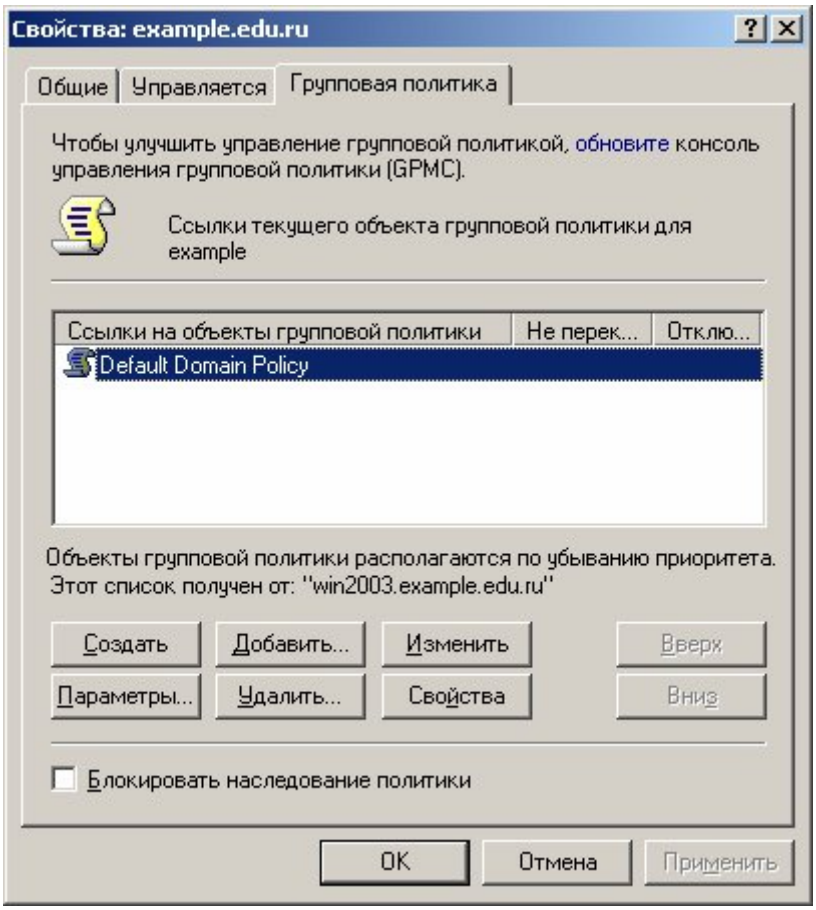

Рисунок 4. Свойства домена.

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики ***Default Domain Policy*** (двойной щелчок по политике);

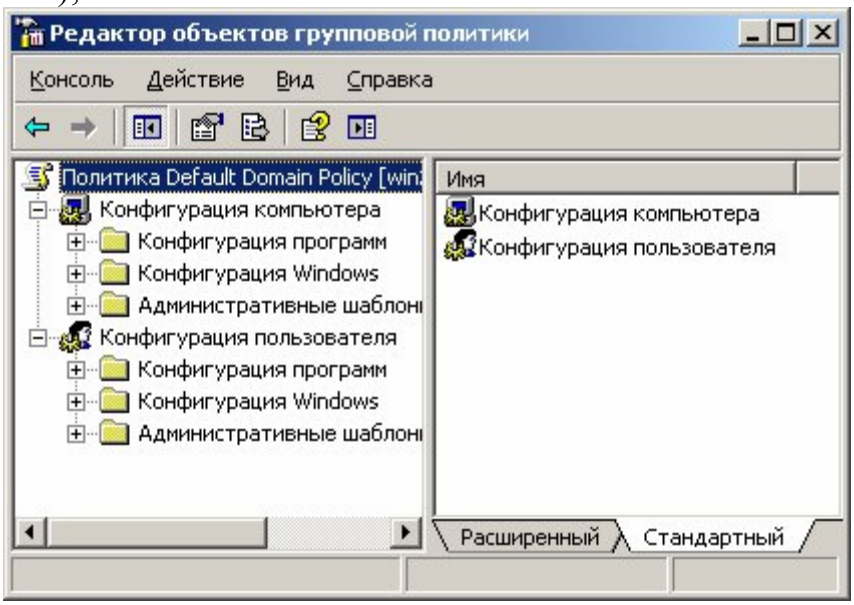

Рисунок 5. Редактор объектов групповой политики

- внесите в изменения в политику паролей:
  - перейдите в раздел **Политика паролей (*Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/ Политики паролей*)**;

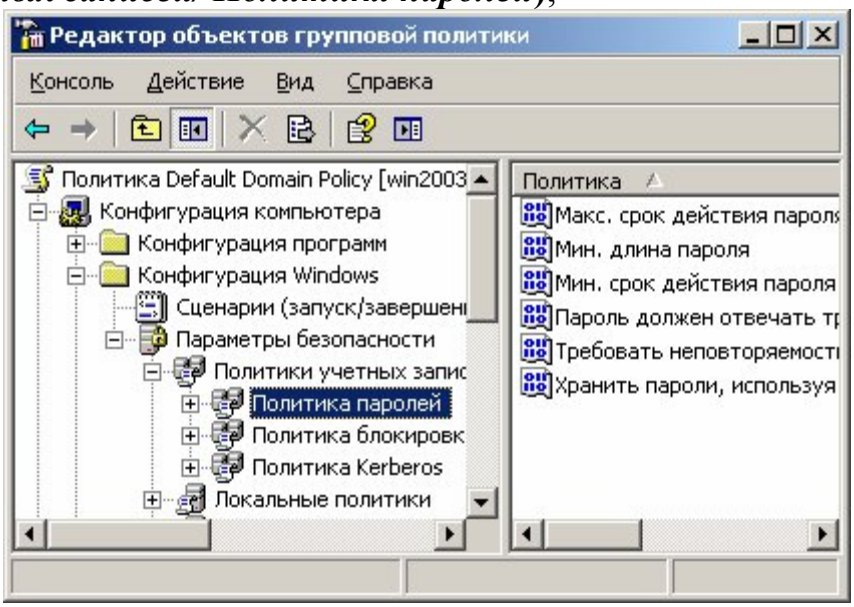

Рисунок 6. Политика паролей.

  - установите минимальную длину пароля:
  - откройте окно **изменения параметров пароля** (двойной щелчок по надписи ***Мин. длинна пароля***);
  - введите в поле **Длина пароля не менее** – *5*;
  - подтвердите изменения кнопкой ***ОК***;
  - отключите соответствие пароля требованиям сложности:
  - откройте диалоговое окно **свойств требования сложности** (двойной щелок по надписи ***Пароль должен отвечать требованиям сложности***);
  - установите радиокнопку *Отключить*;
  - подтвердите изменения кнопкой ***ОК***;
- закройте **Редактор объектов групповой политики (*Консоль/Выход*)**;
- закройте диалоговое окно свойств домена кнопкой ***ОК***.

10. Выполните выход из системы с повторным входом для активации изменений в политике безопасности. *Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.*
11. Измените пароль созданного ранее пользователя:
- активизируйте раздел **Students**;
- задайте новый, более простой пароль пользователю **Просто пользователь**:
  - откройте диалоговое окно **задания пароль (*контекстное меню/Смена пароля*)**;
  - введите в поле **Пароль** – *123*;
  - введите в пол **Подтверждение пароля** – *123*;

Обратите внимание что сообщений о слишком простом пароле не было.

12. Исключите созданного ранее пользователя из группы **group1**:

- откройте диалоговое окно **свойств группы**;
- перейдите на вкладку **Члены группы**;
- выделите в списке удаляемого пользователя и щелкните по кнопке ***Удалить***;
- подтвердите удаление кнопкой ***Да***;
- закройте диалоговое окно свойств группы кнопкой ***ОК***.

13. Включите созданного ранее пользователя в администраторы домена:

- откройте диалоговое окно **свойств пользователя Просто пользователь**;
- перейдите на вкладку **Член групп** и щелкните ***Добавить***;
- введите в поле Администраторы домена;
- завершите добавление в группу кнопкой ***ОК***;
- закройте окно свойств пользователя кнопкой ***ОК***.

Задание 3. Присоединение компьютеров под управлением Windows XP к домену.

1. Запустите виртуальную машину **VM-3** и загрузите в ней ОС **Windows XP**.
2. Откройте диалоговое окно **Свойства системы (*Пуск/Панель управления/Система*)** и перейдите на вкладку **Имя компьютера** (*Далее*).
3. Откройте диалоговое окно **Изменение имени** кнопкой ***Изменить***.
4. Укажите в разделе **Является членом** – *домена*.
5. Введите в поле левую часть имени созданного ранее домена, например **example**.

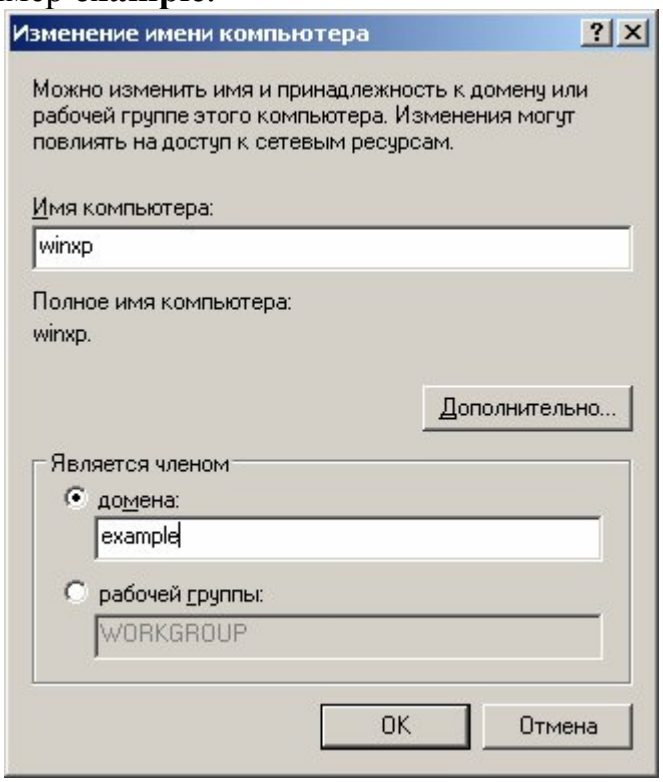

Рисунок 7. Изменение имени компьютера.

6. Подтвердите изменения кнопкой ***ОК***. *Через некоторое время домен к которому подключается компьютер запросит имя и пароль администратора домена.*

7. Введите **имя/пароль** администратора в созданном ранее домене (*JustUser/123*).

8. Ознакомьтесь с сообщением от домена *«Добро пожаловать в домен»* и щелкните ***ОК***.

9. Ознакомьтесь с информацией о необходимости перезагрузки компьютера и закройте окно кнопкой ***ОК***.

10. Закройте диалоговое окно **Свойства системы** кнопкой ***ОК***.

11. В появившемся диалоговом окне согласитесь с перезагрузкой кнопкой ***Да***. *После этого компьютер начнет перезагружаться.*

12. Войдите в систему с использованием любой из созданных вами учетных записей.

13. Проверьте действие сделанных вами ограничений в домене.

14. Выключите ВМ **VM-1**.

Задание 5. Присоединение компьютеров под управлением OpenSUSE Linux к домену.

1. Запустите виртуальную машину **VM-1** и загрузите в ней ОС **OpenSUSE**.

2. Откройте диалоговое окно **Настройки системы (*Главное Меню/Компьютер/YaST Администратор*)**.

3. В появившемся диалоговом окне введите **пароль администратора системы** - *1233456* (задавался при установке системы).

4. Перейдите в раздел **Сетевые службы**.

5. Запустите **Мастер присоединения к домену**

6. В появившемся диалоговом окне подтвердите установку дополнительного пакета **samba-client** кнопкой ***Продолжить***.

7. Введите в поле **Домен или группа** имя созданного ранее домена (левую часть полного имени домена) – *example*.

8. Включите разрешение создания общих ресурсов пользователями.

9. Щелкните по кнопке ***Завершить***.

10. Появится сообщение с предложение присоединить компьютер к домену, щелкните по кнопке ***Да***.

11. Укажите данные администратора домена:
   - введите в поле **Имя пользователя** – *JustUser*;
   - введите в поле **Пароль** – *123*;
   - подтвердите вод данный кнопкой ***Да***.

12. Проверьте правильность подключения к домену:
   - выйдите из системы;
   - войдите в систему под одной из учетных записей пользователей домена.

13. Завершите работу ВМ.

Лабораторная работа 4. Настройка параметров безопасности домена

Цель: научиться устанавливать и просматривать Active Directory, научится подключать компьютеры к домену.

Средства для выполнения работы:

- аппаратные: компьютер;
- программные: ОС Windows 2003 server.

Теоретические сведения

Словосочетание *"информационная безопасность"* в разных контекстах может иметь различный смысл. В **Доктрине информационной безопасности Российской Федерации** термин "информационная безопасность" используется в широком смысле. Имеется в виду состояние защищенности национальных интересов в информационной сфере, определяемых совокупностью сбалансированных интересов личности, общества и государства.

В **Законе РФ "Об участии в международном информационном обмене"** информационная безопасность определяется аналогичным образом – как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Под ***информационной безопасностью*** будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

Комплекс работ по внедрению политики информационной безопасности можно разделить на 3 этапа

На первом этапе определяются общие подходы к политике ИБ, определяются группы ИБ и общее описание разрешений.

На втором этапе осуществляется документирование политики ИБ: составление правил и инструкций для работников организации.

На третьем этапе осуществляется реализация (внедрение) политики ИБ как программными, так и аппаратными средствами.

Следует разработать ряд правил, которые помогут регламентировать работу всех пользователей в сети (как привилегированных так и не привилегированных). В частности следует разработать:

- правила административного обслуживания;
- перечень прав и обязанностей пользователей;
- правила для администраторов;
- правила создания «гостевых» учетных записей.

Разработка таких правил позволит получить ряд преимуществ:

- рутинные задачи всегда выполняются одинаково;
- уменьшение вероятности появления ошибок;
- работа по инструкциям выполняется гораздо быстрее.

Помимо разработки ряда правил для пользователей следует предусмотреть (разработать) стандартные методики:

- подключения и конфигурирования и модернизации компьютеров;
- инсталляции и деинсталляции программного обеспечения;
- резервного копирования данных;
- назначения адресов;
- и т.д.

Например, считается, что управление адресами и именами компьютеров, идентификаторами пользователей и групп должно осуществляться единообразно.

Правила для пользователей

Во многих организациях существуют специально разработанные правила пользователей, только после подписания, которых пользователь получает доступ к сети организации.

В правилах для пользователя необходимо регламентировать такие вопросы:

- использование учетных записей совместно с друзьями и родственниками;
- использование программ дешифровки паролей;
- нарушение нормального процесса обслуживания;
- использование чужих учетных записей;
- использование файлов, чужих учетных записей;
- использование системных ресурсов;
- копирование защищенных авторскими правами материалов;
- возможная незаконная деятельность (мошенничество, клевета и др.).
- вовлечение в деятельность, которая является незаконной.

Правила для администраторов

В правилах для администраторов должны быть сформулированы руководящие принципы использования предоставленных привелегий и соблюдения секретности пользовательских данных. Следует особо отметить использование учетных записей строго индивидуально.

Правила и методики для экстренных случаев

Следует заблаговременно предусмотреть действия при различных нештатных ситуациях. Например, для аварийных ситуаций следует указать лиц с их телефонами, которых надо предупредить в первую очередь. При выходе из строя программного обеспечения можно указать серийные номера для их самостоятельной переустановки или контактную информацию поставщика программного обеспечения.

Безопасность в домене под управлением Windows

Преимущества использования групповой политики:

- При интеграции со службой ***Active Directory*** позволяет как централизованно, так и децентрализовано управлять параметрами безопасности и настройками пользователей.
- Обладает гибкостью и масштабируемостью. Может быть применена в широком наборе конфигураций системы.

• Предоставляет администратору единый инструмент управления с простым и понятным интерфейсом – **Групповая политика**.

• Обладает высокой степенью надежности и безопасности.

Политика безопасности в сети на основе **Windows** храняться в двух типах объектов:

• локальный объект групповой политики;

• объект групповой политики домена.

Для работы с объектами групповой политики используется оснастка **Групповая политика**, которая может запускаться как для локального компьютера, так и для удаленного.

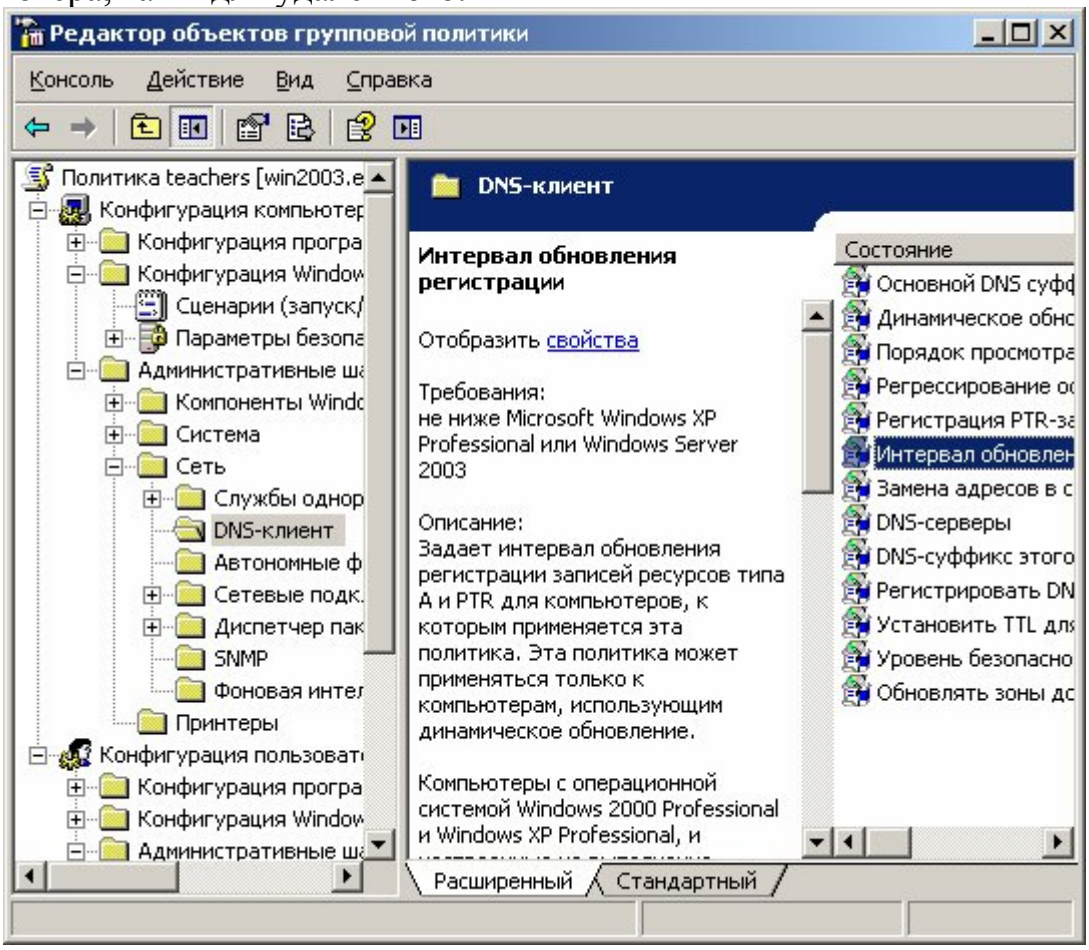

Рисунок 1. Редактор объектов групповой политики.

В структуре объекта групповой политики выделяется 2 раздела (узла):

• *Узел конфигурации компьютера.* Содержит параметры всех политик, определяющих работу компьютера. Они регулируют параметры функционирования операционной системы, определяют права пользователей в системе.

• *Узел конфигурации пользователя.* Содержит параметры всех политик, определяющих работу пользователя на компьютере. Они регулируют вид рабочего стола и конфигурацию рабочей среды, управляют пользовательскими сценариями входа и выхода.

Каждый из перечисленных выше узлов содержит:

• *Административные шаблоны.* Здесь находится групповая политика, определяющая параметры реестра, задающие работу в и внешний вид рабочего стола, компоненты операционной системы и приложений.

• *Параметры безопасности.* Служит для настройки параметров системы безопасности компьютеров: политик аудита и блокировки учетных записей, права пользователя и т.п.

• *Установка программ.* Служит для централизованного управления программным обеспечением организации. С его помощью моэно задать различные режимы установки новых программ на компьютеры пользователей.

• *Сценарии.* Сценарии используются для автоматического выполнения набора команд при загрузке операционной системы и в процессе завершения ее работы.

• *Перенаправление папок.* Позволяет перенаправлять обращение к специальным папкам в сеть.

Выполнение работы

Задание 1. Создайте документы, описывающие политику информационной безопасности для школы, и сохраните их в личной папке.

• правила административного обслуживания;

• перечень прав и обязанностей пользователей;

• правила для администраторов;

• правила создания «гостевых» учетных записей.

Задание 2. Создание и редактирование групповой политики.

1. Откройте диалоговое окно оснастки **Пользователи и компьютеры (*Пуск/Администрирование/Active Direcory – Пользователи и компьютеры*)**.

2. Выполните редактирование политики безопасности домена, созданную автоматически:

- откройте диалоговое окно свойств домена **example.edu.ru (контекстное меню/Свойства)**;
- перейдите на вкладку **Групповая политика**;

В списке будет расположена политика домена по умолчанию Default Domain Policy.

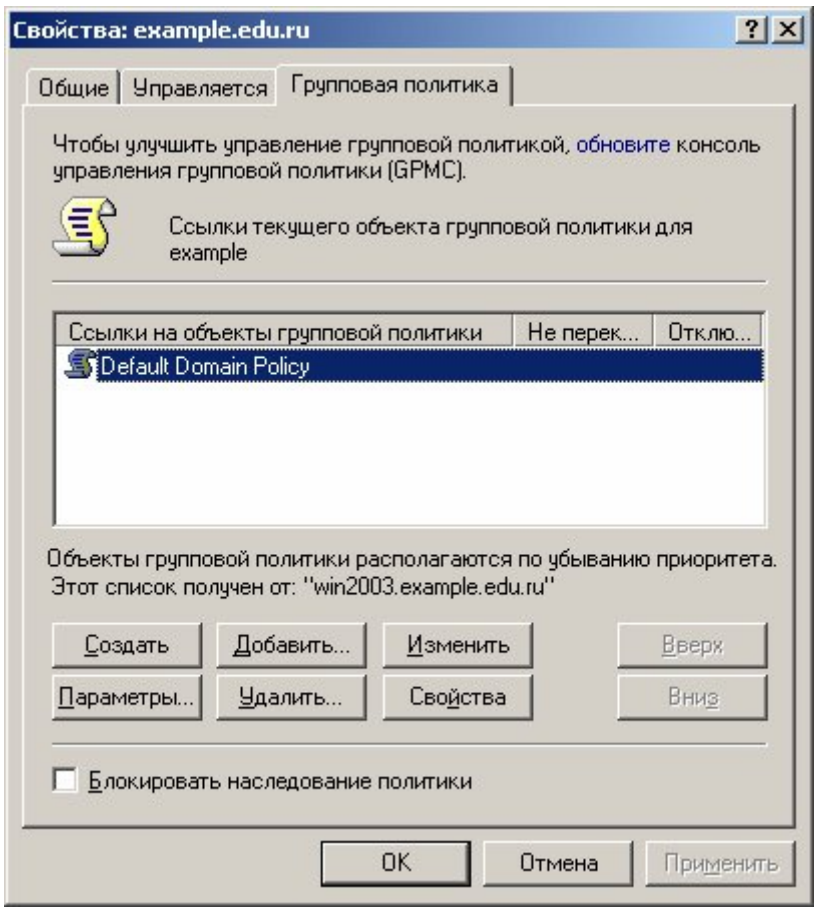

Рисунок 2. Свойства домена.

- откройте диалоговое окно (**Редактор объектов групповой политики**) изменения политики **Default Domain Policy** (двойной щелчок по политике);

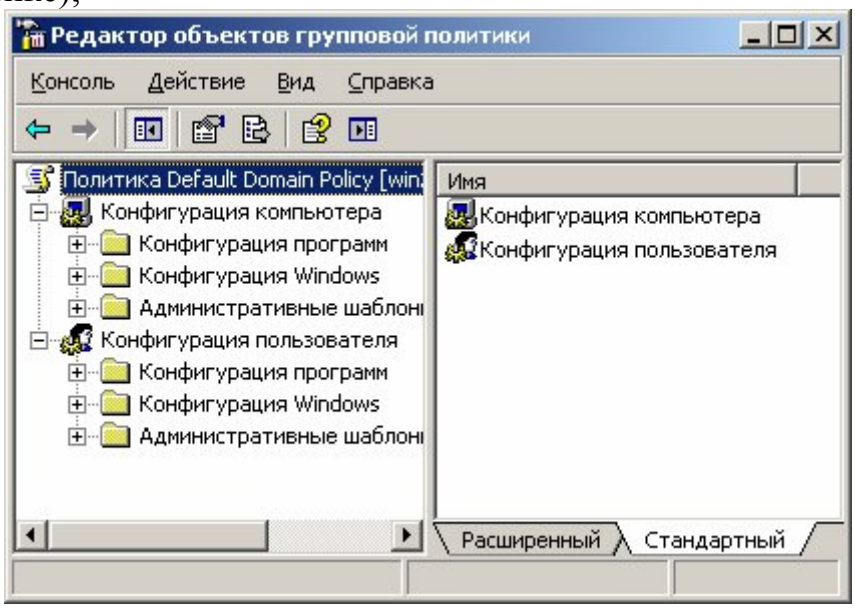

Рисунок 3. Редактор объектов групповой политики.

- внесите в изменения в политику паролей:
  - перейдите в раздел **Политика паролей (*Конфигурация компьютера/Конфигурация Windows/Параметры безопасности/Политики учётных записей/Политики паролей*)**;

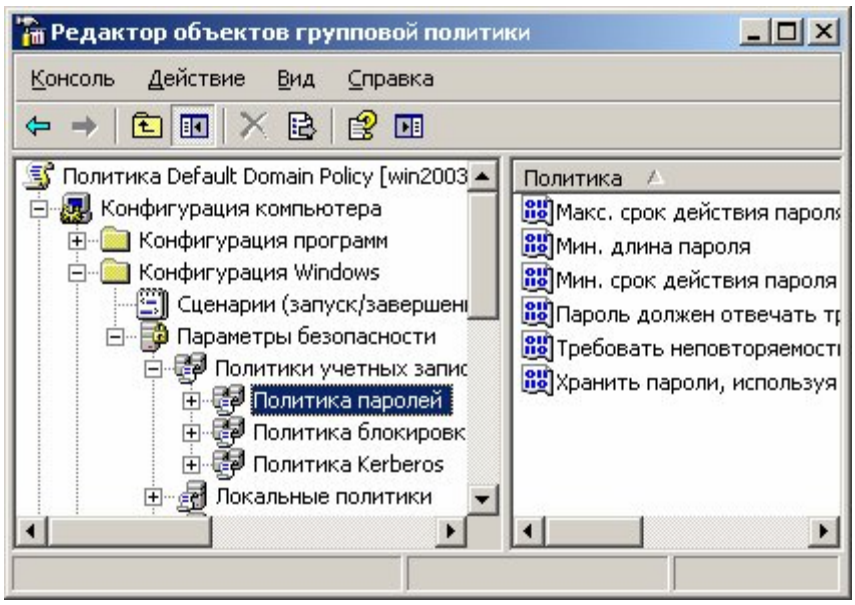

Рисунок 4. Политика паролей.

- установите **минимальную длину пароля**: откройте окно изменения параметров пароля (двойной щелчок по надписи **Мин. длинна пароля**) и введите в поле **Длина пароля не менее**– *5 (**ОК**)*;
- отключите **соответствие пароля требованиям сложности**:
- откройте диалоговое окно свойств требования сложности (двойной щелок по надписи **Пароль должен отвечать требованиям сложности**);
- установите радиокнопку *Отключить*;
- подтвердите изменения кнопкой ***ОК***;
- отключите **возможность использования экранных заставок**:
- перейдите в раздел **Экран (*Конфигурация пользователя/Административные шаблоны/Экран*)**;
- откройте диалоговое окно свойств **Использовать экранные заставки** и выберите *Отключен*;
- подтвердите изменения кнопкой ***ОК***.

- закройте **Редактор объектов групповой политики (*Консоль/Выход*)**;
- закройте диалоговое окно свойств домена кнопкой ***ОК***.

3. Создайте новую политику для учителей:

- откройте диалоговое окно свойств домена **example.edu.ru (*контекстное меню/Свойства*)** и перейдите на вкладку **Групповая политика**;
- активизируйте создание новой политики кнопкой ***Создать***;
- введите название политики - *Teachers*;
- самостоятельно измените созданную политику, отключив пользователям возможность менять фон рабочего стола.

4. Закройте редактор объектов групповой политики.

Задание 3. Создание групп и учетных записей пользователей.

1. Откройте оснастку **Пользователи и компьютеры**.

2. Создайте новую учетную запись пользователя в контейнере **Students**:

- откройте диалоговое окно **Новый объект – Пользователь**, кнопкой ***Создание нового пользователя в текущем контейнере*** ;
- введите данные о пользователе:
  - **Полное имя пользователя** – *Просто Пользователь*;
  - **Имя входа пользователя (логин)** – *JustUser*;
  - Подтвердите введенные данные кнопкой ***Далее***.

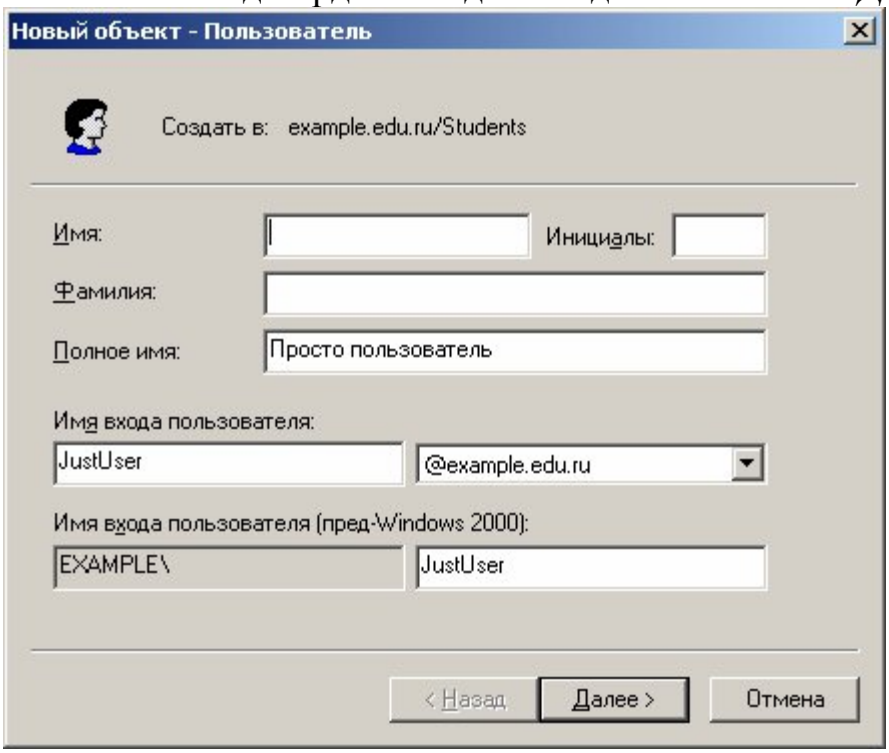

Рисунок 5. Ввод данных нового пользователя.

- установите пароль для пользователя:
  - введите в поле **Пароль** – *User1234*;
  - введите в поле **Подтверждение** – *User1234*;
  - установите флажок *Срок действия пароля не ограничен*;
  - завершите ввод пароля кнопкой ***Далее***.

В правой области отобразиться запись, соответствующая созданному пользователю.

3. Введите более полную информацию о пользователе:

- откройте диалоговое окно свойств пользователя (двойной щелчок по надписи **Просто пользователь**);
- введите в поле **Описание** – *это тестовый пользователь*;
- введите в поле **Комната** - номер кабинета в котором проходит занятие - *316*;
- введите в поле **Телефон** – <номер своего мобильного телефона>;
- укажите адресные данные на вкладке **Адрес**;
- укажите несколько дополнительных телефонов пользователя на вкладке **Телефоны**;

- завершите изменение данных пользователя кнопкой ***ОК***.

4. Создайте группу **group1** в контейнере **Students**:

- откройте диалоговое окно создания групп (***контекстное меню/Создать/Группа***);
- введите **имя группы – *group1*;**
- **завершите создание группы кнопкой *ОК*.**

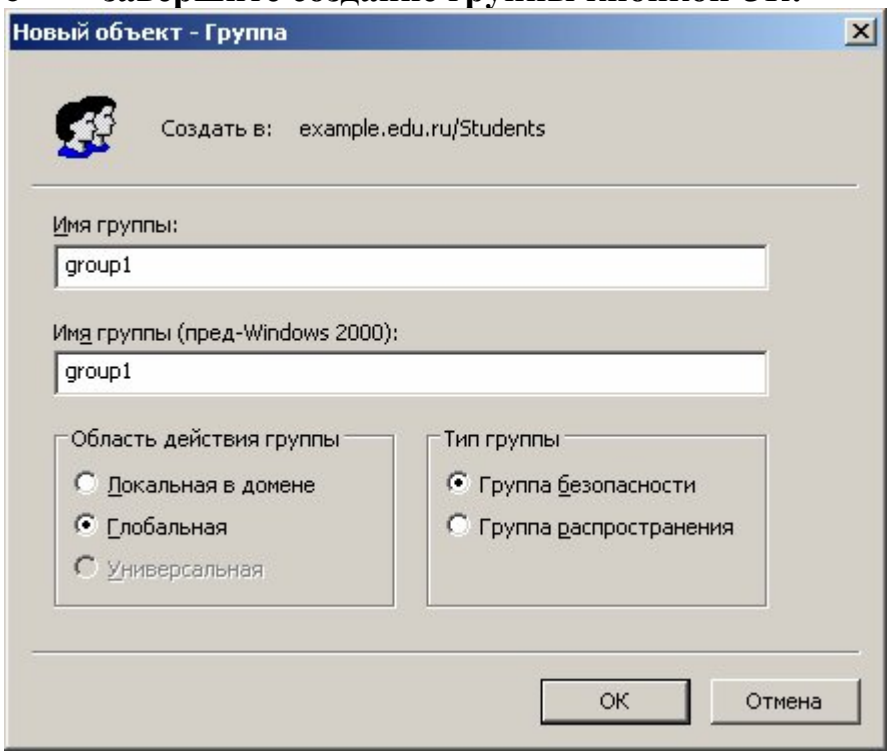

Рисунок 6. Создание группы.

5. Задайте дополнительную информацию для группы group1:

- **откройте диалоговое окно свойств группы (*двойной щелчок по надписи group1*);**
- **введите в поле Описание – *Это тестовая группа*;**
- **завершите изменение данных группы кнопкой *ОК*.**

6. Включите созданного ранее пользователя *Просто пользователь (JustUser)* в группу group1:

- **откройте диалоговое окно свойств пользователя (*двойной щелчок по записи пользователя*);**
- **перейдите на вкладку Член групп;**
- **откройте диалоговое окно выбора группы кнопкой *Добавить*;**
- **введите название группы – *group1*;**
- **завершите добавления пользователя в группу кнопкой *ОК*.**
- **закройте диалоговое окно свойств пользователя кнопкой *ОК*.**

7. **Выполните выход из системы с повторным входом для активации изменений в политике безопасности.** ***Изменения в политике паролей вступят в силу только после выхода из системы и повторного входа в неё.***

8.

9. Измените пароль созданного ранее пользователя:

- **активизируйте раздел Students;**
- **задайте новый, более простой пароль пользователю Просто пользователь:**
  - **откройте диалоговое окно задания пароль (*контекстное меню/Смена пароля*);**
  - **введите в поле Пароль – *123*;**
  - **введите в пол Подтверждение пароля – *123*;**

Обратите внимание что сообщений по слишком простом пароле не было.

-

10. Исключите созданного ранее пользователя из группы group1:

- **откройте диалоговое окно свойств группы;**
- **перейдите на вкладку Члены группы;**
- **выделите в списке удаляемого пользователя и щелкните по кнопке *Удалить*;**
- **подтвердите удаление кнопкой *Да*;**
- **закройте диалоговое окно свойств группы кнопкой *ОК*.**

11. Включите созданного ранее пользователя в администраторы домена:

- **откройте диалоговое окно свойств пользователя Просто пользователь;**
- **перейдите на вкладку Член групп и щелкните *Добавить*;**
- **введите в поле *Администраторы домена*;**
- **завершите добавление в группу кнопкой *ОК*;**
- **закройте окно свойств пользователя кнопкой *ОК*.**

12. **Закройте оснастку Пользователи и компьютеры.**

Лабораторная работа 5. Работа с серверами http и ftp

Цель: научиться устанавливать и просматривать ***Active Directory***, научится подключать компьютеры к домену.

Средства для выполнения работы:

• аппаратные: компьютер;

• программные: Виртуальная машина: VM-2; Сервер FTP : **Filezilla**; Образ установочного диска: win2003-1.iso, win2003-2.iso.

Теоретические сведения

Сервер - в локальных вычислительных сетях - специализированная ЭВМ, управляющая использованием разделяемых между терминалами сети дорогостоящих ресурсов системы.

Сервер (англ. *server* от англ. *to serve* — служить) — в информационных технологиях — программный компонент вычислительной системы, выполняющий сервисные функции по запросу клиента, предоставляя ему доступ к определённым ресурсам.

Сервер сети (*Server*) - это компьютер, подключенный к сети и предоставляющий пользователям сети определенные услуги, например, хранение данных общего пользования, печать заданий, обработка запроса к СУБД, удаленная обработка заданий и т.д. Сервер работает по заданиям клиентов. После выполнения задания сервер посылает полученные результаты клиенту, инициировавшему это задание.

Обычно связь между клиентом и сервером поддерживается посредством передачи сообщений, и при этом используется определенный протокол для кодирования запросов клиента и ответов сервера. Виды серверов: FTP; Файловый; Web; Телефонный; Терминальный; Факс; Суперсервер и т.д.

Файл-серверы представляют собой серверы для обеспечения доступа к файлам на диске сервера. Прежде всего это серверы передачи файлов по заказу, по протоколам **FTP и HTTP**. Протокол**HTTP** ориентирован на передачу текстовых файлов, но серверы могут отдавать в качестве запрошенных файлов и произвольные данные, например динамически созданные веб-страницы, картинки, музыку и т. п. *Другие серверы* позволяют монтировать дисковые разделы сервера в дисковое пространство клиента и полноценно работать с файлами на них. Это позволяют серверы протоколов **NFS и SMB**. Серверы **NFS и SMB** работают через интерфейс **RPC**.

Недостатки файл-серверной системы:

• Очень большая нагрузка на сеть, повышенные требования к пропускной способности. На практике это делает практически невозможной одновременную работу большого числа пользователей с большими объемами данных.

• Обработка данных осуществляется на компьютере пользователей. Это влечет повышенные требования к аппаратному обеспечению каждого пользователя. Чем больше пользователей, тем больше денег придется потратить на оснащение их компьютеров.

• Блокировка данных при редактировании одним пользователем делает невозможной работу с этими данными других пользователей.

• Безопасность. Для обеспечения возможности работы с такой системой Вам будет необходимо дать каждому пользователю полный доступ к целому файлу, в котором его может интересовать только одно поле

Файловый сервер выполняет следующие функции:

• хранение данных,

• архивирование данных,

• согласование изменений данных, выполняемых разными пользователями,

• передача данных.

FTP-сервер - это понятие, за которым скрывается обычный компьютер. Но так как он содержит общедоступные файлы и настроен на поддержку протокола **FTP**, то его называют сервером - поставщиком информации. *FTP-клиент* - это сервисная программа, с помощью которой можно произвести соединение с **FTP** сервером. Обычно эта программа имеет командную строку,

но некоторые имеют оконный интерфейс и не требуют запоминания команд. *WEB-сервер* необходим для обслуживания WEB-страниц вашего сайта

Доступ к WEB-серверу имеет пять уровней:

1. Общедоступный с возможностью только чтения всех **URL** за исключением тех, что помещены в каталогах ***/private***.
2. Доступ сотрудников организации, которой принадлежит сервер. Здесь также допустимо только чтение, но доступны и секции каталога ***/private***.
3. Разработчики **WEB-сервера**. Имеют возможность модифицировать содержимое сервера, инсталлировать CGI-скрипты, прерывать работу сервера.
4. Администраторы узла (сервера). Имеют те же привилегии, что и разработчики, но могут также реконфигурировать сервер и определять категорию доступа.
5. Системные администраторы. Имеют идентичные привилегии с администраторами сервера.

Оснастка Internet Information Service (IIS) обеспечивает средства управления сервером для контроля над доступом и содержимым веб-узлов и узлов **FTP**. Например, разработчикам это средство позволит выполнить доскональную проверку работы узла перед окончательной загрузкой на сервер интрасети организации или Интернета. Оснастка **IIS** имеет следующие особенности:

- дополнительные параметры настройки сервера, в частности, для управления узлом **FTP**, независимого выполнения приложений, настройки типов **MIME** и назначения дополнительных средств обработки сценариев.
- мастер создания виртуальных каталогов.
- возможность управления установками **Internet Information Services** в сети.

На сегодняшний день существует огромное множество программного обеспечения для работы с протоколом **FTP** под все операционные системы. Все это множество программного обеспечения можно разделить на две части: *серверное ПО* и *клиентское ПО*. *Серверное ПО* служит для создания и управления ftp-сервером. *Клиентское ПО* используется для просмотра ресурсов на ftp-сервере. Этот класс программ призван обеспечить комфортную работу с удаленными ресурсами. Сюда относятся такие программы как:

- **ftp.exe** – стандартное приложение **Windows**;
- **FileZilla** – мощный ftp-клиент с открытым исходным кодом (т.е. при желание вы можете что-нибудь новое добавить в эту программу самостоятельно);
- **RigthFTP, CuteFTP** – графические ftp-клиенты;
- **Total commander** (или любой другой с интерфейсом **Norton Commander**)– имеет встроенный ftp клиент;
- **Explorer.exe** – стандартное приложение **Windows**;
- Любой браузер.

Выполнение работы

Задание 1. Подготовьте файловый сервер.

1. Подключите к виртуальной машине **VM-2** образ установочного диска ***win2003-2.iso***.

2. Запустите виртуальную машину **VM-2**.

3. Добавьте новую **роль** серверу – *Файл-сервер*:

- откройте диалоговое окно **Управление данным сервером (*Пуск/дминистрирование/Управление Данным Сервером*)**;
- активизируйте добавление ролей кнопкой ***Добавить или удалить роль***;
- выберите **Файловый сервер** и щелкните ***Далее***;
- установите параметры файлового сервера:
  - Предоставить доступ UNIX-системам к файлам;
  - Предоставить доступ Apple--системам к файлам;
  - подтвердите введенные параметры кнопкой ***Далее***;
- запустите установку роли сервера кнопкой ***Далее***.

4. Перезагрузите виртуальный компьютер кнопкой ***Перезегрузить***.

5. Откройте диалоговое окно **Настройки файлового сервера (*Пуск/дминистрирование/Управление Данным Сервером/Управление этим файловым сервером*)**.

6. Установите стандартные квоты использования места на диске:

- установите флажок *Установить дисковые квоты по умолчанию для новых пользователей данного сервера*;
- укажите **размер квот** - *50Мб*;
- установите **предупреждение о квоте** - *40Мб*;
- установите флажок *Не выделять место на диске при превышении дискового пространства*;
- завершите ввод стандартных квот кнопкой ***Далее***.

7. Откажитесь от включения службы индексирования.

8. Укажите папку на сервере, для хранения файлов, например ***C:\Documents and settings\Администратор\Рабочий стол\PUB***.

9. Далее мастер установки завершит свою работу. Попробуйте теперь зайти на созданную вами сетевую папку с другого компьютера сети. Обратите внимание на способ подключения. Попробуйте заполнить папку для превышения квоты.

Задание 2. Настройте Web-сервер.

1. Установите **Internet Information Service (IIS) (*Пуск/администрирование/Управление Данным Сервером/Сервер приложений IIS*)**:

2. Подготовьте тестовую страницу:

- создайте временную страницу, вызываемую по умолчанию: наберите в **Блокноте** и сохраните в файле с именем ***Default.html*** в

каталоге ***\Inetpub\wwwroot***.

```
<HTML>
	<HEAD>
		<TITLE>Тестовая страница<TITLE>
	</HEAD>
<BODY>
	<H1 align="center"> Тестовая страница </H1>
	<P align="center">
		<FONT color="green">
			На этом месте будет размещена страница нашей организации. В настоя
			</FONT>
	</P>
</BODY>
</HTML>
```

-
3. Настройте **Web-сервер**:
   - откройте консоль управления сервером **IIS (*Пуск/администрирование/Управление Данным Сервером/Управление этим сервером приложений*)**;
   - перейдите к web-узлу, заданному по умолчанию (***Диспетчер служб IIS/Веб-узлы/Веб-узел по умолчанию***);

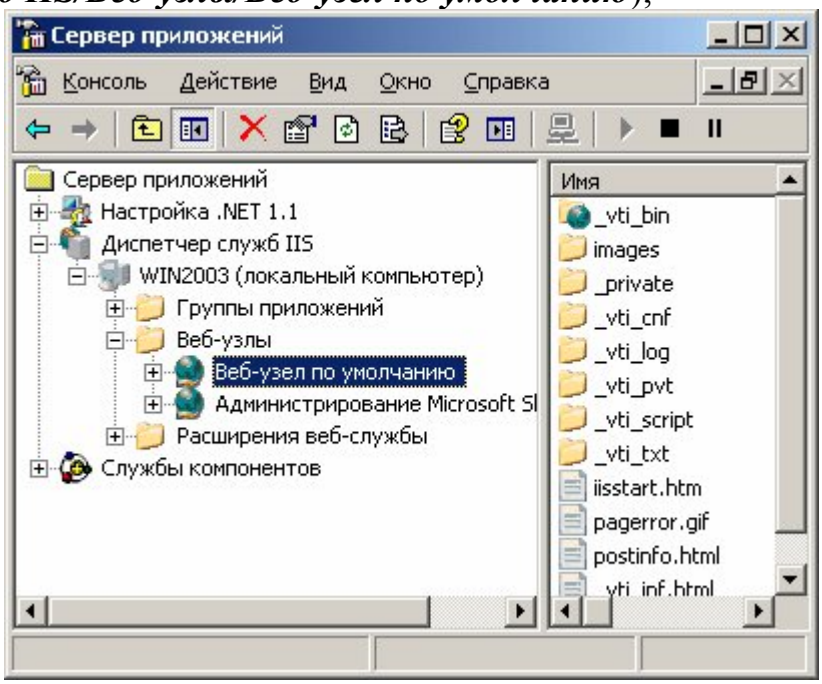

Рисунок 1. Консоль управления сервером приложений (IIS).

   - откройте диалоговое окно **Свойства узла по умолчанию (*контекстное меню/Свойства*)**;
   - добавьте страницу по умолчанию:
     - перейдите на вкладку **Документы**;
     - установите флажок *Задать страницу содержания по умолчанию*;
     - откройте окно добавления кнопкой ***Добавить***;

- введите в поле ***Default.html***;
- подтвердите добавление кнопкой ***OK***.

- закройте окно свойств кнопкой ***OK***.

4. Проверьте настройку **Web-сервера**:

- на вашем компьютере откройте **Internet Explorer (*Пуск/Программы/Internet Explorer*)**;
- наберите в адресной строке **http://127.0.01/**;
- сделайте скриншот происходящего на экране и сохраните его в своей папке.

Задание 3. Установите и настройте сервер FTP

1. Установите сервер **FTP - FileZilla**.
2. Запустите **FileZilla Server Interface**.

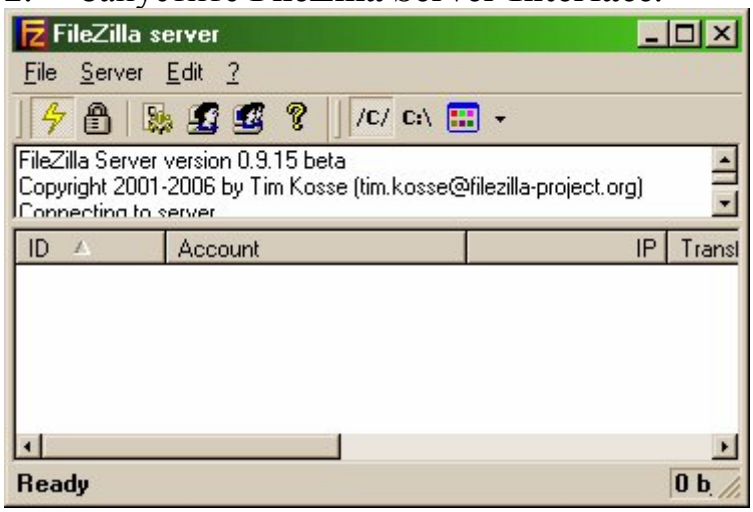

*Рисунок 2. Интерфейс управления FTP-сервером **FileZilla***

3. Ограничьте количество одновременных подключений к серверу:

- откройте окно настройки сервера (***Edit/Settings***);

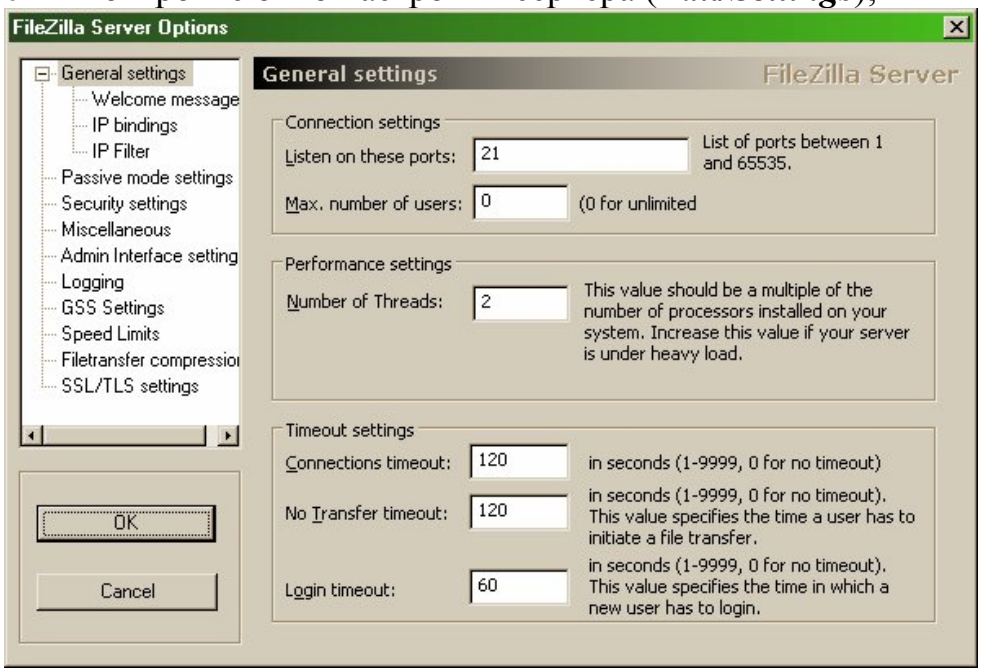

Рисунок 3. Настройки FTP-сервера

- перейдите в раздел **General Settings** (общие настройки);

- введитевполе **Max.number of users** – *2*;

4. Установите текст приветствия:

- перейдите в раздел **Welcome message**;
- введите в поле **Custom welcome message** – *Добро пожаловать на мой сервер*;

▪ Установите ограничения по скорости:

▪ перейдите в раздел **Speed Limits** (ограничения скорости);

▪ включите использование правил ограничения скорости радиокнопкой *Use Speed Limit rules*;

▪ добавьте ограничение по скорости не более 3 Кб/с в понедельник:

▪ откройте окно задания параметров ограничений кнопкой ***Add*** (Добавить);

▪ сбросьте все флажки кроме *Monday* (Понедельник);

▪ введите в поле **Speed** – *3*;

▪ подтвердите ввод данных кнопкой ***OK***;

▪ примените параметры кнопкой ***OK***.

▪ Создайте группы пользователей **FTP-сервера**:

▪ откройте диалоговое окно **добавления групп** кнопкой на панели инструментов;

▪ активируйте добавление групп кнопкой ***Add*** (Добавить);

▪ введите **имя группы**, например *Students* (***OK***);

▪ задайте общую папку для созданной группы:

▪ перейдите в раздел **Shared Folders** (Общие папки);

▪ активируйте добавление папок кнопкой ***Add*** (Добавить);

▪ укажите общую папку, например ***C:\Documents and settings\Администратор\Рабочий стол*** и подтвердите выбор кнопкой ***OK***;

▪ разрешите чтение и удаление содержимого общей папки – установите флажок *Write и Delete*;

▪ завершите добавление групп пользователей кнопкой ***OK***.

▪ Добавьте нового пользователя:

▪ откройте диалоговое окно добавления пользователей кнопкой на панели инструментов;

▪ активируйте добавление пользователей кнопкой ***Add*** (Добавить);

▪ введите **имя группы**, например *justuser*;

▪ выберите в списке **User should be member of the following group** созданную ранее группу и подтвердите создание пользователя кнопкой ***OK***;

▪ установите пароль для созданного пользователя:

▪ перейдите на вкладку **General** (Общие);

▪ введите в поле **Password** новый пароль, например *123*;

▪ завершите добавление групп пользователей кнопкой ***OK***.

▪ Проверьте работу сервер:

▪ запустите командную строку (***Пуск/Программы/Стандартные/Командная строка***);

- введите команду для подключения к FTP-серверу на текущем компьютере: **FTP 127.0.0.1**
- введите имя пользователя - *justuser* (***ENTER***);
- введите пароль - *123* (***ENTER***);
- просмотрите содержимое домашней папки: **DIR**
- отключитесь от сервера: **QUIT**
- закройте командную строку.
- Закройте интерфейс управления **FTP-сервером**.

Лабораторная работа 6. Мониторинг состояния элементов сети

Цель: научится устанавливать операцционную систему Windows на компьютер.

Средства для выполнения работы:

• аппаратные: компьютер с установленной ОС Windows XP.

• программные: приложения ВМ: VirtualBox; виртуальные машины: VM-1, VM-2.

Теоретические сведения

Системная служба **Журнал событий** запускается по умолчанию при загрузке операционной системы и регистрирует события в трех журналах (в зависимости от роли сервера журналов может быть больше):

• *Приложение* (содержит информацию об изменении конфигурации в системе);

• *Система* (содержит данные о системных событиях);

• *Безопасность* (содержит записи о событиях входа в систему и о доступе к ресурсам).

Для мониторинга и оптимизации работы компьютера в системах **Windows Server 2003** имеется несколько инструментов, позволяющих администратору следить за работой любых компонентов системы и конфигурировать ее оптимальным образом. Эти инструменты перечислены ниже.

• ***Task Manager (Диспетчер задач)*** служит для просмотра текущих данных о производительности системы. В этой утилите основными являются три индикатора: использование процессора, использование виртуальной памяти и запущенные процессы и программы.

• ***Оснастка Event Viewer (Просмотр событий)*** позволяет просматривать журналы событий, генерируемых приложениями, службой безопасности и системой.

• ***Performance (Производительность)*** – обновленная оснастка систем **Windows XP** и **Windows Server 2003**, аналог утилиты ***Performance Monitor*** в **Windows NT 4.0.** Оснастка ***Performance***включает в себя два компонента: *ActiveX-элемент System Monitor* и оснастку *Performance Logs and Alerts* (Оповещения и журналы безопасности). Графические средства *System Monitor* позволяют визуально отслеживать изменение производительности системы. С помощью *System Monitor* можно одновременно просматривать данные с нескольких компьютеров в виде динамических диаграмм, на которых отображается текущее состояние системы и показания счетчиков. Оснастка *Performance Logs and Alerts* позволяет создавать отчеты на основе текущих данных производительности или информации из журналов. При превышении счетчиками заданного значения или уменьшения нижеуказанного уровня данная оснастка посредством службы сообщений (Messenger) посылает оповещения пользователю.

Диспетчер задач можно использовать для отслеживания ключевых индикаторов производительности компьютера, он позволяет определять статус

запущенных программ и завершать приложения, которые перестали отвечать на запросы системы. С помощью диспетчера задач можно отслеживать активность запущенных процессов по 25 параметрам и просматривать графики использования процессора и памяти.

В **Windows Server 2003** диспетчер задач содержит пять вкладок/индикаторов. Ниже перечислены эти вкладки и указано их назначение.

• *Applications (Приложения)* – показывает статус приложений, запущенных на компьютере.

• *Processes (Процессы)* – содержит информацию о процессах, запущенных на компьютере.

• *Performance (Быстродействие)* – отображает динамическое состояние производительности компьютера, включая степень использования памяти и процессора.

• *Networking (Сеть)* – показывает степень загрузки сети. Индикатор отображается только при наличии на компьютере сетевой карты.

• *Users (Пользователи)* – содержит список зарегистрированных пользователей. Эти пользователи могут регистрироваться локально (с консоли) или являться клиентами служб *Terminal Services*, подключенных с использованием технологий *Terminal Server, Remote Access* или *Remote Assistant*.

В операционных системах **Windows** событием называется любое значительное "происшествие" в работе системы или приложения, о котором следует уведомить пользователей. В случае возникновения критических событий, таких как переполнение диска сервера или неполадки с электропитанием, на экран монитора будет выведено соответствующее сообщение. Остальные события, которые не требуют немедленных действий от пользователя, регистрируются в системных журналах. Служба регистрации событий в системных журналах активизируется автоматически при каждом запуске системы **Windows Server 2003**.

Оснастка Event Viewer

В системе **Windows Server 2003** для просмотра системных журналов можно использовать оснастку ***Event Viewer (Просмотр событий)*** (группа ***Administr-tive Tools (Администрирование)*** на панели управления). Эту оснастку можно также запустить из окна оснастки ***Computer Management (Управление компьютером)***. На рис. 1 показан пример окна оснастки ***Event Viewer*** для контроллера домена.

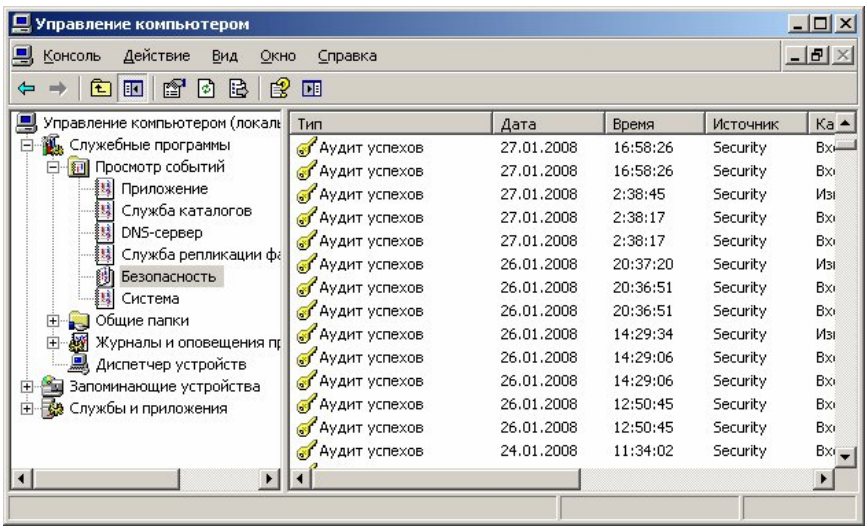

Рисунок. 1. Окно оснастки Event Viewer.

Оснастку ***Event Viewer*** можно также открыть с помощью команды ***Пуск/Программы/Администрирование/Просмотр событий***. С помощью оснастки ***Event Viewer*** можно просматривать три типа стандартных (основных) журналов.

• *Журнал приложений (Application log)* — фиксирует события, зарегистрированные приложениями. Например, текстовый редактор может зарегистрировать в данном журнале ошибку при открытии файла.

• *Журнал системы (System log)* — записывает события, которые регистрируются системными компонентами **Windows Server 2003**. Например, в системный журнал записываются такие события, как сбой в процессе загрузки драйвера или другого системного компонента при запуске системы.

• *Журнал безопасности (Security log)* — содержит записи, связанные с системой безопасности. С помощью этого журнала можно отслеживать изменения в системе безопасности и идентифицировать бреши в защите. В данном журнале можно регистрировать попытки входа в систему. Для просмотра журнала необходимо иметь права администратора. По умолчанию регистрация событий в журнале безопасности отключена.

Помимо стандартных, на компьютере — в первую очередь на контроллере домена — могут быть и другие журналы, создаваемые различными службами (например, ***Active Directory, DNS, File Replication Service*** и т. д.). Работа с такими журналами ничем не отличается от процедур просмотра стандартных журналов.

Журнал системы безопасности может просматривать только пользователь с правами системного администратора. По умолчанию регистрация событий в данном журнале отключена. Для запуска регистрации необходимо установить политику аудита.

Типы событий, регистрирующихся в журналах:

• *Error (Ошибка)* — событие регистрируется в случае возникновения серьезного события (такого как потеря данных или функциональных возможностей). Событие данного типа будет зарегистрировано, если невозможно загрузить какой-либо из сервисов в ходе запуска системы.

• *Warning (Предупреждение)* — событие не является серьезным, но может привести к возникновению проблем в будущем. Например, если недостаточно дискового пространства, то будет зарегистрировано предупреждение.

• *Information (Уведомление)* — значимое событие, которое свидетельствует об успешном завершении операции приложением, драйвером или сервисом. Такое событие может, например, зарегистрировать успешно загрузившийся сетевой драйвер.

• *Success Audit (Аудит успехов)* — событие, связанное с безопасностью системы. Примером такого события является успешная попытка регистрации пользователя в системе.

• *Failure Audit (Аудит отказов)* — событие связано с безопасностью системы. Например, такое событие будет зарегистрировано, если попытка доступа пользователя к сетевому диску закончилась неудачей.

Информация о событиях содержит следующие параметры:

• *Параметр* - Описание

• *Type (Тип)* -Тип события

• *Date (Дата)* - Дата генерации события

• *Time (Время)* - Время регистрации события

• *Source (Источник)* - Источник (имя программы, системного компонента или компонента приложения), который привел к регистрации события

• *Category (Категория)* - Классификация события по источнику, вызвавшему его появление

• *Event ID (Событие)* - Идентификатор события

• *User (Пользователь)* - Учетная запись пользователя, от имени которой производились действия, вызвавшие генерацию события

• *Computer (Компьютер)* - Компьютер, на котором зарегистрировано событие

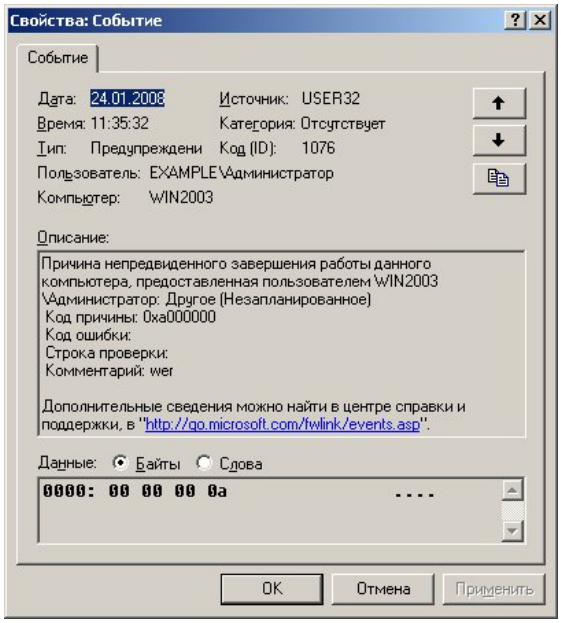

Рисунок. 2. Дополнительная информация о событии.

Для просмотра дополнительной информации о событии выберите в меню ***Action (Действие)*** пункт ***Properties (Свойства)*** (либо щелкните дважды

кнопкой мыши на строке в списке событий). Появится окно, пример которого показан на рис. 2. На панели **Description (Описание)** приведена общая информация о событии. На панели **Data (Данные)** отображаются двоичные данные, которые могут быть представлены как *Bytes (Байты)* или как *Words (Слова)*. Эти данные могут быть интерпретированы опытным программистом или техническим специалистом службы поддержки, знакомым с исходным кодом приложения.

Выполнение работы

Задание 1. Просмотрите сетевые подключения к компьютеру.

1. Подготовьтесь к выполнению задания:
   - запустите виртуальную машину **VM-2**;
   - создайте на рабочем столе общую папку ***MyFolder*** и разместите в ней документ с именем ***CompName.doc***, содержащий сведения об IP-адресе и символьном имени компьютера;
   - переключитесь в обычный компьютер и откройте документ ***CompName.doc***. Для этого воспользуйтесь **Сетевым окружением**.

Все остальные операции следует выполнять на виртуальном компьютере, где был создан файл ***CompName.doc****.*

2. Переключитесь в виртуальную машину **VM-2**.
3. Откройте оснастку **Управление компьютером (*контекстное меню значка Мой компьютер/Управление*)**.
4. Разверните раздел **Общие ресурсы**. *Здесь перечислены все опубликованные (общие) ресурсы вашего компьютера.*
5. Отключите общий доступ к созданному ранее ресурсу ***MyFolder***. Для этого в контекстном меню ресурса выберите *Прекратить общий доступ*.
6. Откройте раздел **Сеансы**.
7. Здесь перечислены все открытые сеансы, т.е. какие пользователи и на каких компьютерах сейчас подключены к вашему компьютеру. Если вызвать контекстное меню раздела, то можно сразу отключить все сеансы.
8. Закройте открытый файл. Для этого перейдите в раздел **Открытые файлы** и в контекстном меню файла выберите *Закрыть открытый файл*.

Задание 2 Отключите пользователя с отправкой ему уведомления.

1. Подготовьтесь к выполнению задания. Для этого откройте на обычном компьютере файл ***CompName.doc***, расположенные в виртуальной машине **VM-2**.
2. Переключитесь в виртуальную машину;
3. Откройте оснастку **Управление компьютером**.
4. Выполните для элемента **Общие ресурсы** команду ***контекстного меню/ Все задачи/Отправка сообщения консоли***.
5. Введите в поле **Сообщение** текст выводимого сообщения: *Вы сейчас будете отключены от общего ресурса* и щелкните по кнопке ***Отправить***.
6. Закройте окно **Отправка сообщений консоли**.
7. Для раздела **Открытые файлы** выполните команду контекстного меню ***Отключить все открытые файлы***.
8. Просмотрите пришедшее сообщение.

Задание 3. Просмотрите сведения о процессах системы и ее состоянии.

1. Просмотрите информацию о производительности системы:
   - откройте окно диспетчера задач (**CTRL+SHIFT+ESC**);
   - перейдите на вкладку **Процессы**;

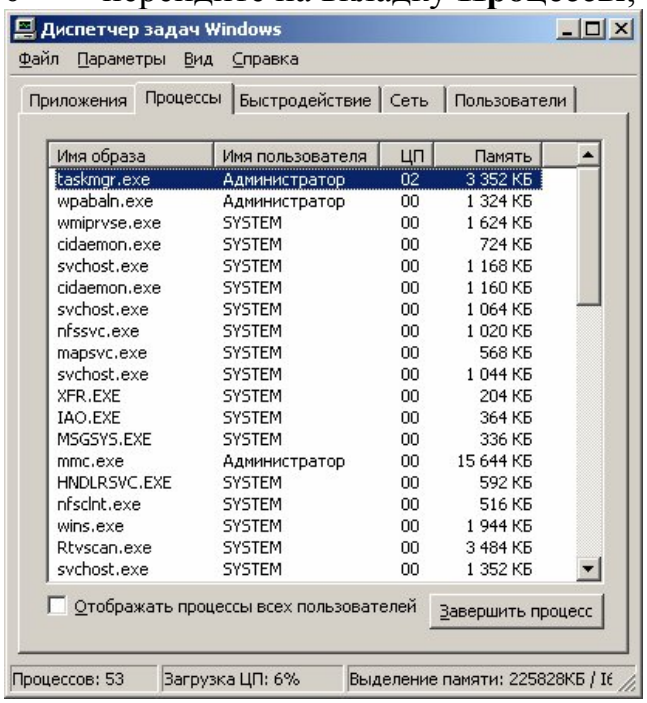

Рисунок 3. Диспетчер задач.

   - просмотрите список и найдите процесс использующий наибольшее количество памяти;
   - перейдите на вкладку **Быстродействие** и посмотрите количество выделенной памяти в соответствующем поле;
   - перейдите на вкладку **Сеть** и ознакомьтесь с информацией о производительности сети;
   - перейдите на вкладку **Пользователи** просмотрите информацию о пользователях, зарегистрированных в системе.

2. Соберите с помощью **Диспетчера задач** информацию, указанную ниже:

Количество запущенных приложений.
Имя процесса, занимающего больше всех оперативной памяти.
Количество выделенной памяти.
Имя пользователя зарегистрированного в системе.

3. Сохраните полученную информацию в личном каталоге в файле формата **ODT**.

Задание 4. Выполните мониторинг сетевых подключений.

1. Запустите оснастку **Производительность** (***Пуск/Администрирование/Проивзводительность***).

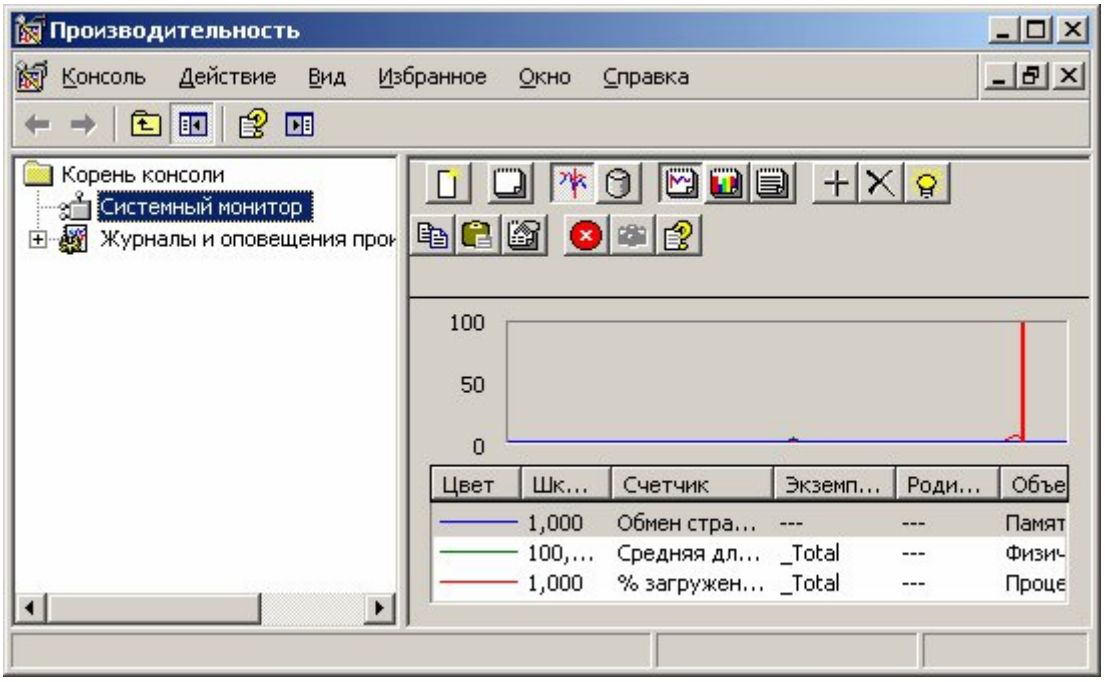

Рисунок 4. Оснастка Производительность

2. Удалите все счетчики из системного монитора:
   - активируйте **Системный монитор** в левой части окна **Производительность**;
   - откройте диалоговое окно свойств **Системного монитора** кнопкой ***Свойства*** ;
   - перейдите на вкладку **Данные**;
   - выделите один из счетчиков и удалите его кнопкой ***Удалить***;
   - аналогично удалите все остальные счетчики.
3. Добавьте счетчик активных подключений TCP:
   - активируйте добавление счетчика кнопкой ***Добавить***;
   - выберите в раскрывающемся списке **Объект** – *TCPv4*;
   - выберите в списке **Выбрать счетчик из списка** – *Активных подключений*;
   - просмотрите информацию о добавляемом счетчике, щелкнув по кнопке ***Объяснение***;
   - добавьте счетчик кнопкой ***Добавить***.

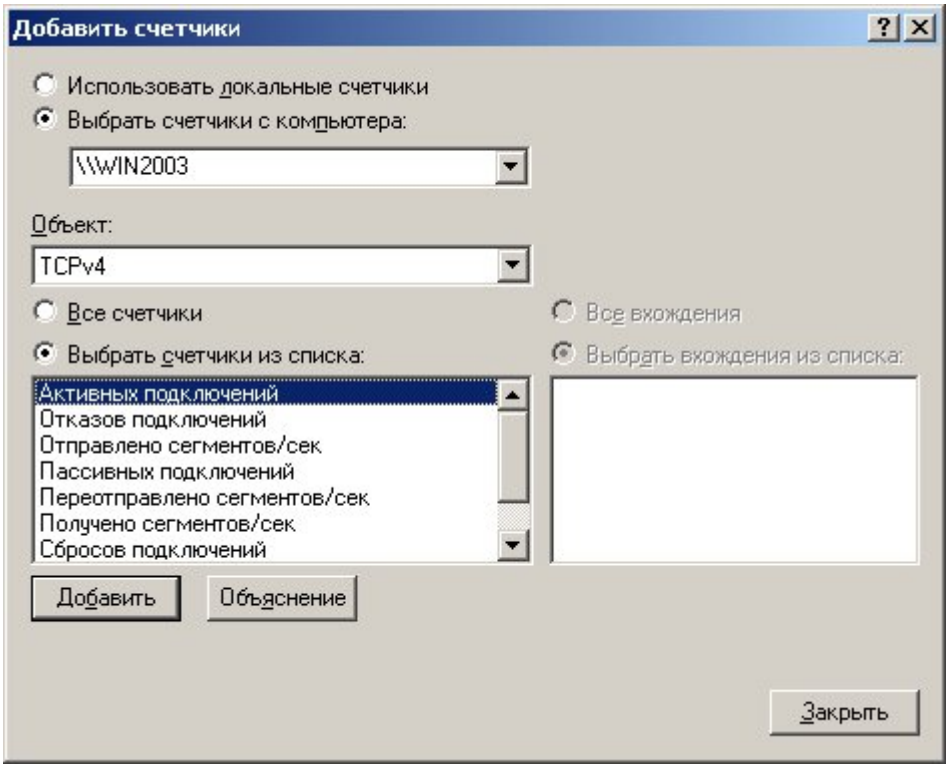

Рисунок 5. Добавление счетчика.

- самостоятельно добавьте счетчик ***Всего байт/сек*** для объекта ***Сервер***;
- закройте окно добавления счетчиков кнопкой ***Закрыть***.

4. Закройте диалоговое окно свойств **Системного монитора** кнопкой ***ОК***.

В правой области начнет отображаться информация добавленных счетчиков в графическом виде.

5. Переключите вид отображения информации счетчиков в текстовый вид кнопкой ***Просмотр отчета*** на панели инструментов.

6. Настройте автоматический сбор информации о загруженности сервера в период **с** 8.00 **до** 17.00:

- активируйте раздел **Журналы счетчиков** в левой части окна **Производительность**;
- активируйте создание новых параметров журнала (***Действие/Новые параметры журнала***);
- введите название журнала в поле **Имя** - *Дневная нагрузка* и подтвердите кнопкой ***ОК***;
- добавьте объект **Сервер**:
  - откройте окно добавления объектов кнопкой ***Добавить объект***;
  - выделите в списке **Объект** – *Сервер*;
  - добавьте объект кнопкой ***Добавить***;
  - закройте окно добавления объектов кнопкой ***Закрыть***;
- аналогично добавьте объект **Сетевой интерфейс**;
- установите время сбора данных:
  - перейдите на вкладку **Расписание**;

- установите в поле **Время** – *8.00*;
- установите время остановки – *17.00*;

- закройте диалоговое окно параметров нового журнала кнопкой ***ОК***. *В правой части окна* ***Производительность*** *появится новый журнал. Просмотреть результат работы журнала можно в папке* ***C:\perflogs***.

7. Настройте оповещение, если количество доступной памяти станет менее ***100 Мб***.

- активируйте раздел **Оповещения** в левой части оснастки **Производительность**;
- откройте диалоговое окно **Новые параметры оповещения** (***Действия/Новые параметры оповещения***);
- введите **имя новых параметров** - *Мало памяти* и подтвердите ввод кнопкой ***ОК***;

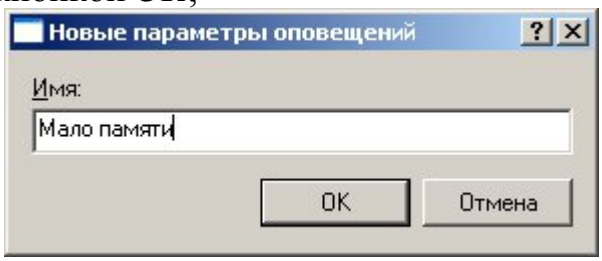

Рисунок 6. Ввод имени новых параметров оповещения.

- введите в поле **Комментарий** – *Оповещение о малом количестве оперативной памяти*;
- добавьте счетчик ***Доступно МБ*** для объекта **Память**;
- введите в поле **Порог** значение, при котором должно срабатывать оповещение – *100*;

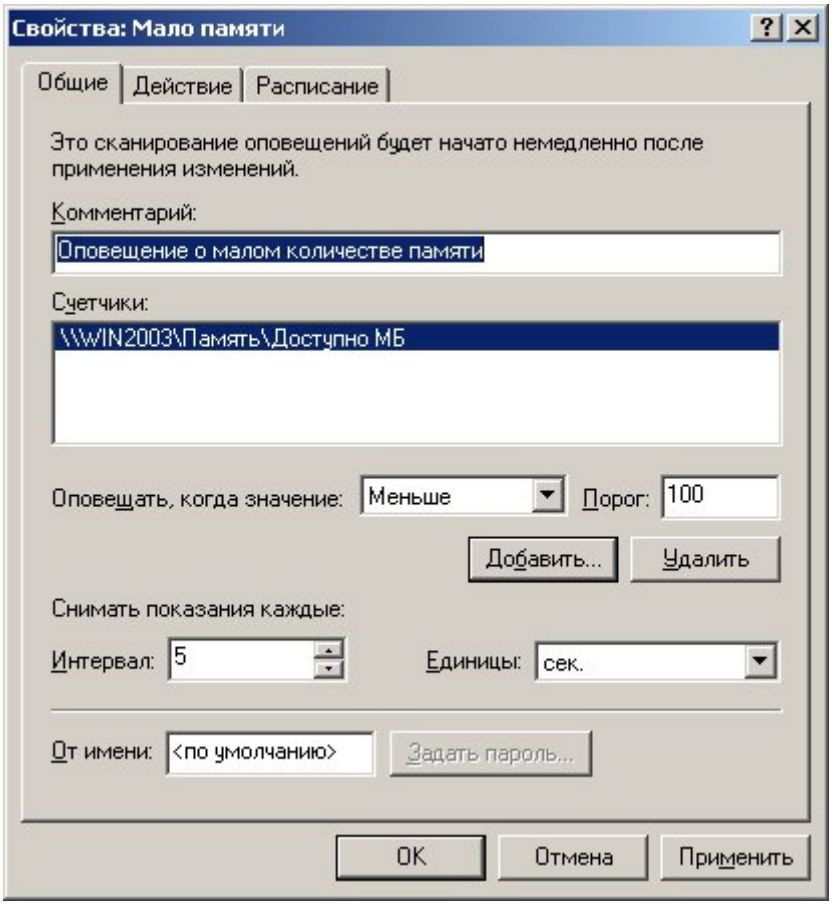

Рисунок 7. Установка параметров оповещения.

- задайте действие, которое должно срабатывать при установленном условии:
  - перейдите на вкладку **Действие**;
  - установите флажок *Послать сетевое сообщение* и введите в поле текст сообщения - *Слишком мало памяти*;
- завершите настройку оповещения кнопкой ***ОК***.

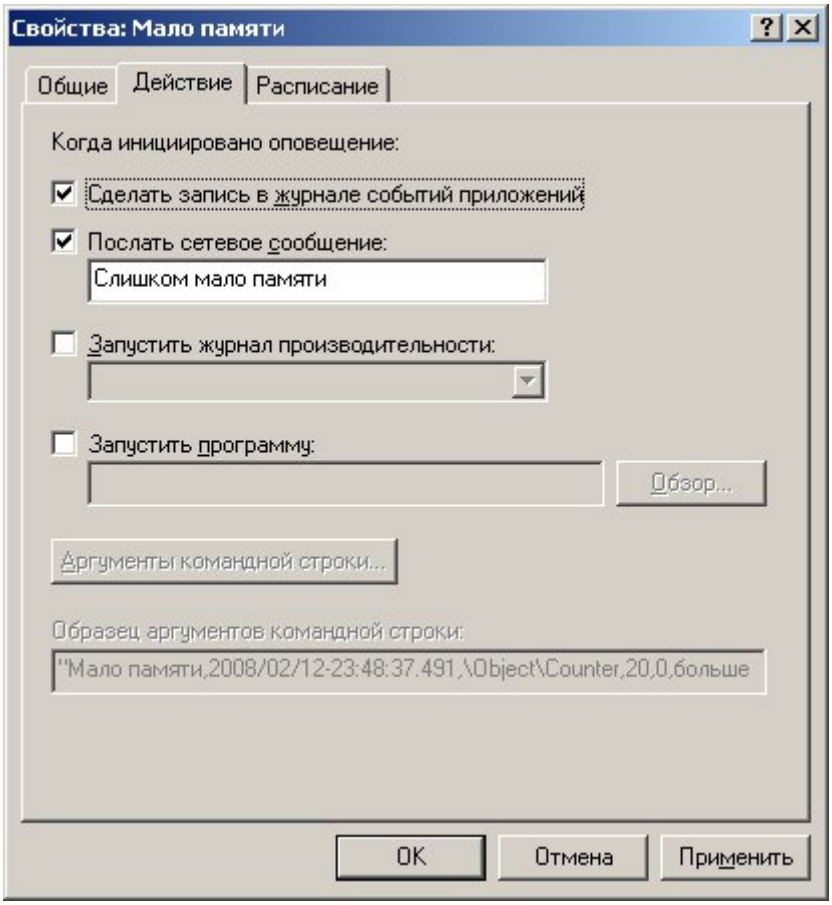

Рисунок 8. Диалоговое окно свойств параметров оповещения.

Задание 5. Выполните просмотр событий.

1. Откройте оснастку **Управление компьютером** (***Пуск/Администрирование/Управление компьютером***).
2. Разверните узел **Просмотр событий**.

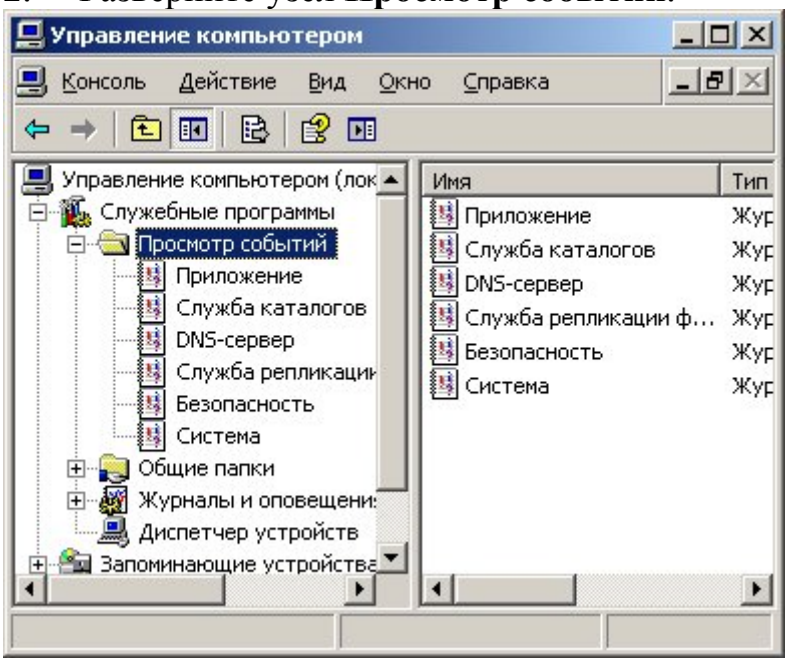

Рисунок 9. Диалоговое окно Просмотр событий.

3. Просмотрите события ***Службы безопасности***:

- перейдите в раздел **Безопасность** в левой части оснастки **Управление компьютером**;

Справа отобразятся все события данной службы.

- выполните фильтрацию событий только для пользователя ***JustUser***:
  - откройте диалоговое окно свойств раздела **Безопасность** (***Действия/Свойства***);
  - перейдите на вкладку **Фильтр**;

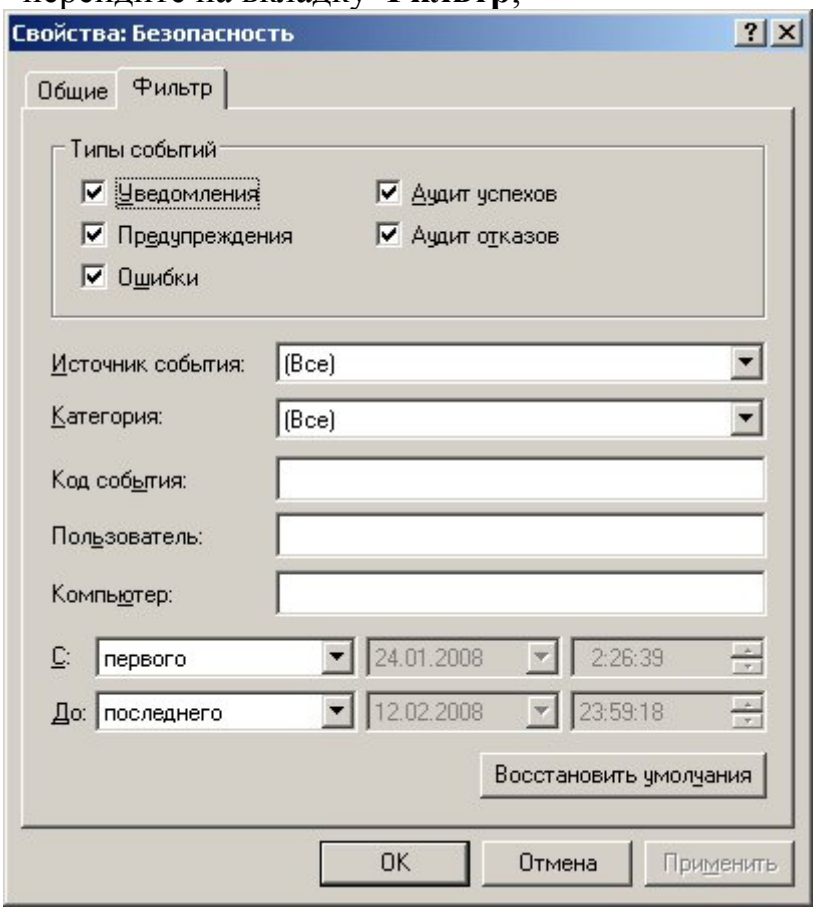

Рисунок 10. Диалоговое окно Фильтр.

  - введите в поле **Пользователь** имя пользователя, для которого необходимо отобразить события, например *JustUser*;
  - самостоятельно установите в полях **С** и **ДО** сегодняшний день;
  - подтвердите применение фильтра кнопкой ***ОК***.
- просмотрите событие ***Доступ к службе каталогов***:
  - найдите указанное событие в правой части окна оснастки **Управление компьютером**;
  - откройте диалоговое **окно свойств** выбранного события (***Действия/Свойства***);
  - ознакомьтесь с информацией события, найдите имя компьютера к которому осуществлялся доступ;
  - закройте диалоговое окно свойств события кнопкой ***ОК***.

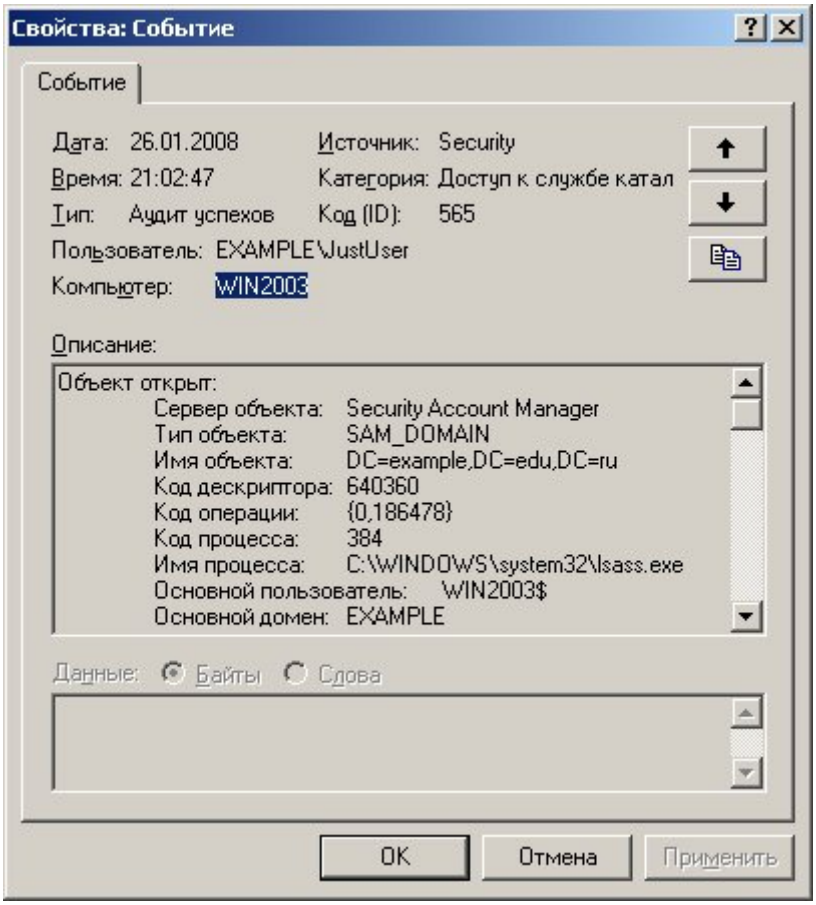

Рисунок 11. Диалоговое окно Свойства события.

- снимите установленный ранее фильтр:
  - откройте диалоговое **окно свойств** раздела **Безопасность**;
  - прейдите на вкладку **Фильтр**;
  - восстановите стандартные значения кнопкой ***Восстановить умолчания***;
  - закройте диалоговое окно свойств раздела **Безопасность** кнопкой ***ОК***.

4. Экспортируйте список событий для раздела **DNS-сервер** в текстовый файл:
   - активизируйте раздел **DNS-сервер**;
   - откройте **диалоговое окно экспорта** (***Действие/Экспортировать список***);
   - введите *имя файла* в поле **Имя**;
   - сохраните файл кнопкой ***Сохранить***;
   - просмотрите сохраненный файл стандартной программой ***Блокнот***.

Лабораторная работа 7. Настройка параметров безопасности Интернет браузера

Цель: научиться настраивать параметры безопасности в современных Интернет браузерах.

Средства для выполнения работы:

• аппаратные: компьютер

• программные: ОС Windows XP или Windows 2000; браузеры: Internet Explorer; Firefox, Opera.

Теоретические сведения

Компьютер, подсоединенный к сети Интернет, может подвергнуться реальным атакам. *Основные опасности при работе в сети Интернет* с помощью браузера следующие:

• переносимые программы (ActiveX и Java-апплеты) внедренные в web_страницу;

• языки сценариев (JavaScript и VBScript), которые призваны превратить статичное содержимое HTML-страницы в динамическое.

• cookie, сохраняемые браузером могут позволить заинтересованным лицам следить за Вашими действиями в сети и знать о Ваших интересах.

Современные веб-страницы часто содержат небольшие программы: *Java-апплеты*, управляющие элементы *ActiveX*, скрипты *JavaScript*. Загрузка и выполнение таких переносимых программ, очевидно, связаны с большим риском возникновения массовых атак. Разработаны различные методы, направленные на минимизацию этого риска.

Java-апплеты – это программы на языке Java, откомпилированные в машинный язык, которые размещаются на веб-странице и загружаются вместе с ней. Апплеты обрабатываются интерпретатором **JVM (*Java Virtual Machine* —** виртуальная машина Java) в браузере, как показано на рисунке 1.

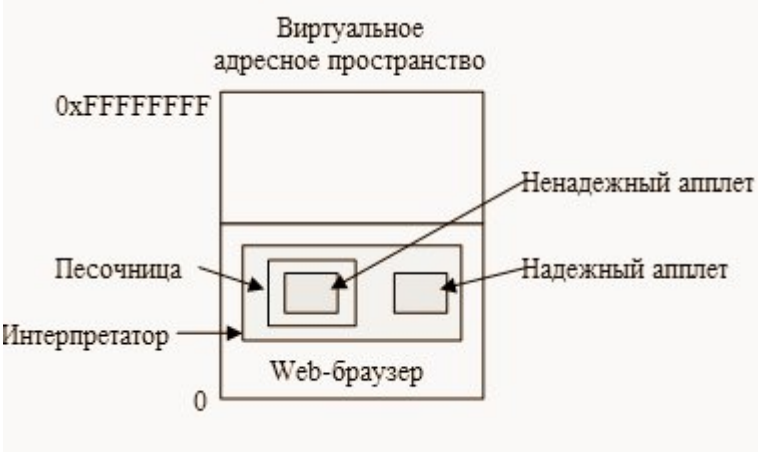

Рисунок 1. Обработка апплетов браузером

Преимущество интерпретируемого кода перед компилируемым состоит в том, что перед его исполнением изучается каждая инструкция. Это дает интерпретатору возможность проверить состоятельность адреса инструкции. Кроме того, системные вызовы также перехватываются и интерпретируются. Как именно они обрабатываются, зависит от политики защиты информации.

• если апплет *надежный* (например, он был создан на локальном диске), его системные вызовы могут обрабатываться без дополнительных проверок;

• если апплет *не может считаться надежным* (например, он был загружен из Интернета), его можно поместить в так называемую песочницу, регулирующую его поведение и пресекающую его попытки использовать системные ресурсы;

• если апплет *пытается захватить системный ресурс*, вызов передается монитору безопасности, который может разрешить или запретить данное действие. Монитор исследует вызов с точки зрения локальной политики защиты информации и затем принимает решение.

Таким образом, можно предоставить апплетам доступ к некоторым (но не ко всем) ресурсам.

Управляющие элементы ActiveX — двоичные программы, которые можно внедрять в веб-страницы. Когда на странице встречается такая программа, производится проверка необходимости ее выполнения, и в случае положительного ответа она запускается. Эти программы не интерпретируются и не помещаются в песочницы, поэтому они обладают такими же возможностями, как обычные пользовательские программы, и, в принципе, могут нанести большой вред. Таким образом, вся защита информации в данном случае сводится к вопросу о том, стоит ли запускать управляющий элемент.

Для принятия таких решений корпорацией Microsoft был выбран метод, базирующийся на подписях кода (*система Authenticode*). Суть в том, что каждый элемент *ActiveX* снабжается цифровой подписью, а именно *хэшем кода*, подписанным его создателем с использованием открытого ключа. Когда браузер встречает управляющий элемент, он сначала проверяет правильность подписи, убеждаясь в том, что код не был заменен по дороге. Если подпись корректна, браузер проверяет по своим внутренним таблицам, можно ли доверять создателю программы. Если создатель надежный, программа выполняется, в противном случае игнорируется. Поскольку нет никакой возможности проследить за деятельностью всех компаний, пишущих переносимые программы, вскоре метод подписания кода может представлять собой довольно серьезную угрозу.

В *JavaScript* вообще отсутствует какая-либо официальная модель системы защиты информации. Каждый производитель пытается что-нибудь придумать. Например, в ***Netscape Navigator 2.0*** было реализовано нечто подобное Java-модели, а в четвертой версии прослеживаются черты модели подписей кода.

В обозревателе ***Internet Explorer*** имеется несколько возможностей, позволяющих обеспечить защиту конфиденциальности, а также повысить безопасность личных данных пользователя.

Параметры конфиденциальности позволяют защитить личные данные пользователя – с помощью этих параметров можно понять, как просматриваемые web-узлы используют эти данные, а также задать значения параметров конфиденциальности, которые будут определять, разрешено ли web-узлам сохранять файлы *cookie* на компьютере.

К *параметрам конфиденциальности* ***Internet Explorer*** относят следующие:

• *параметры конфиденциальности*, определяющие обработку на компьютере файлов cookie.

• *оповещения безопасности*, выдаваемые пользователю при попытке получить доступ к web-узлу, не соответствующему заданным параметрам конфиденциальности;

• *возможность просмотра политики конфиденциальности* стандарта P3P (***Platform for Privacy Preferences***) для web-узла.

Средства безопасности позволяют предотвратить доступ других пользователей к таким сведениям, на доступ к которым у них нет разрешения. Это, например, сведения о кредитной карточке, вводимые при покупках в Интернете, от небезопасного программного обеспечения.

Когда производится загрузка или запуск программ, полученных из Интернета, необходимо убедиться, что программа получена из известного, надежного источника. В связи с этим, при выполнении загрузки на компьютер программы из Интернета, обозреватель ***Internet Explorer*** использует для проверки ее подлинности технологию ***Microsoft Authenticode***, проверяющую наличие у программы действующего сертификата. Следует отметить, что эта мера не препятствует загрузке и запуску на компьютере программ, разработанных с ошибками, но снижает риск использования фальсифицированной программы.

Цифровая подпись — это способ введения электронной метки для файла данных. В этом случае файл подписывается его создателем (издателем). Наличие цифровой подписи позволяет сделать следующие выводы: имеется имя издателя файла, и этот файл не был изменен с тех пор, как он был подписан. При любой попытке фальсификации подпись становится недействительной.

Виды цифровых подписей:

• подписи с симметричным ключом;

• подписи с открытым ключом.

В *первом случае* суть метода состоит в создании некоего центрального авторитетного органа, которому все доверяют. Затем каждый пользователь выбирает секретный ключ и лично относит его в офис этого авторитетного органа. Когда возникает необходимость послать открытым текстом подписанное сообщение, оно (сообщение) шифруется ключом. Затем сообщение посылается в авторитетный орган, который расшифровывает его и посылает получателю со своей собственной подписью. Этим авторитетный орган подтверждает, что сообщение подлинное.

Во *втором случае* ключ делится на две части: закрытая и открытая части. С помощью закрытой части можно подписать данные, причем это может сделать только владелец ключа, а с помощью открытой части можно проверить подпись.

Сертификат – цифровой документ, широко используемый для проверки подлинности и безопасного обмена данными в открытых сетях, таких как

Интернет, экстрасети и интрасети. Сертификат связывает открытый ключ с объектом, хранящим соответствующий закрытый ключ. Сертификаты имеют цифровые подписи, поставленные выдавшими центрами сертификации, и могут предоставляться пользователю, компьютеру или службе. Наиболее широко применяемый формат для цифровых сертификатов определяется международным стандартом ITU-T X.509 версии 3.

Выполнение работы

Задание 1. Настройте параметры безопасности браузера Internet Explorer:

1. Откройте диалоговое окно **Свойства: Интернет (*Пуск/Панель управления/Свойства обозревателя*)**;
2. Перейдите на вкладку **Безопасность** и откройте параметры зоны Интернет с помощью кнопки ***Другой…***;
3. Установите ***Проверку имени пользователя*** в режим **Запрос имени пользователя и пароля**;
4. Разрешите в соответствующих полях указанные ниже действия:
   - Блокировать всплывающие окна;
   - Доступ к источникам данных за пределами домена;
   - Переход между кадрами через разные домены;
5. Установите **Разрешения канала программного обеспечения** на *Высокий уровень безопасности*;
6. Отключите *Использование элементов ActiveX не помеченных как безопасные*;
7. Отключите загрузку *Неподписанных элементов ActiveX*;
8. Примените параметры кнопкой ***ОК***;
9. Установите параметры конфиденциальности:
   - перейдите на вкладку **Конфиденциальность**;
   - установите регулятор на уровень *Умеренно высокий*;
   - разрешите загружать файлы ***cookie*** с узла **www.mail.ru**:
     - щелкните по кнопке ***Узлы***;
     - введите в поле *www.mail.ru* и щелкните по кнопке ***Разрешить***;
   - аналогично разрешите загружать cookie со следующих узлов: **www.yandex.ru, www.pochta.ru**;
   - примените параметры кнопкой ***ОК***;
10. Настройте ограничения на доступ к ресурсам по содержанию информации на них:
    - перейдите на вкладку **Содержание** и откройте окно **Ограничение доступа** кнопкой ***Включить*** в разделе **Ограничения доступа**;
    - установите пароль:
      - перейдите на вкладку **Общие**;
      - откройте окно создания пароля кнопкой ***Создать пароль***;
      - введите **пароль** - *user* и **подсказку** к нему - *user*;
      - примените параметры кнопкой ***ОК***.

- перейдите на вкладку **Оценки** и установите уровни **Службы оценки Recreational Software Advisory Council** по своему усмотрению;
- примените параметры кнопкой ***ОК***;
- очистите пароли, которые браузер автоматически запоминает. Для этого на вкладке **Содержание**, щелкните по кнопке ***Автозаполнение***, а затем по кнопке ***Очистить пароли***;
- удалите временные фалы Интернет и ***cookies*** на вкладке **Общие**.

Лабораторная работа 8. Технология защиты сетевых компьютеров. Брандмауэр.

Цель: научиться защищать сетевой компьютер и настраивать брандмауэр.

Средства для выполнения работы:

• аппаратные: компьютер, подключенный к ЛВС;

• программные: ОС Windows XP; приложение ВМ: VirtualBox; виртуальная машина: VM-1.

Теоретические сведения

Особенности защиты информации в компьютерных сетях обусловлены тем, что сети, обладая несомненными преимуществами обработки информации, по сравнению с локальными компьютерами, усложняют организацию защиты, образуя следующие основные проблемные направления:

1. Разделение совместно используемых ресурсов.
2. Расширение зоны контроля.
3. Комбинация различных программно-аппаратных средств.
4. Неизвестный периметр.
5. Множество точек атаки.
6. Сложность управления и контроля доступа к системе.

Сообществом Интернета под эгидой ***Тематической группы по технологии Интернета (Internet Engineering Task Force, IETF)*** разработано много рекомендаций по отдельным аспектам сетевой безопасности, тем не менее, целостной концепции или архитектуры безопасности пока не предложено.

Основная идея состоит в том, чтобы средствами оконечных систем обеспечивать сквозную безопасность.

Экранирование - единственный сервис безопасности, для которого Гостехкомиссия России одной из первых в мире разработала и ввела в действие **Руководящий документ**, основные идеи которого получили международное признание и фигурируют в профилях защиты, имеющих официальный статус в таких странах, как США. Политика безопасности межсетевого экрана базируется на принципе «все, что не разрешено, запрещено»

Межсетевой экран или *Брандмауэр* — это «полупроницаемая мембрана», которая располагается между защищаемым внутренним сегментом сети и внешней сетью или другими сегментами сети интранет и контролирует все информационные потоки во внутренний сегмент и из него. *Контроль трафика* состоит в его фильтрации, то есть выборочном пропускании через экран, а иногда и с выполнением специальных преобразований и формированием извещений для отправителя, если его данным в пропуске было отказано. Фильтрация осуществляется на основании набора условий, предварительно загруженных в брандмауэр и отражающих концепцию информационной безопасности корпорации. Брандмауэры могут быть выполнены как в виде аппаратного, так и программного комплекса, записанного в коммутирующее устройство или сервер доступа (сервер-шлюз,

прокси-сервер, хост-компьютер и т. д.). Работа брандмауэра заключается в анализе структуры и содержимого информационных пакетов, поступающих из внешней сети, и в зависимости от результатов анализа пропуска пакетов во внутреннюю сеть (сегмент сети) или полное их отфильтровывание. Эффективность работы межсетевого экрана обусловлена тем, что он полностью переписывает реализуемый стек протоколов TCP/IP, и поэтому нарушить его работу с помощью искажения протоколов внешней сети (что часто делается хакерами) невозможно.

Межсетевые экраны обычно выполняют следующие функции:

- физическое отделение рабочих станций и серверов внутреннего сегмента сети (внутренней подсети) от внешних каналов связи;
- многоэтапная идентификация запросов, поступающих в сеть (идентификация серверов, узлов связи и прочих компонентов внешней сети);
- проверка полномочий и прав доступа пользователей к внутренним ресурсам сети;
- регистрация всех запросов к компонентам внутренней подсети извне;
- контроль целостности программного обеспечения и данных;
- экономия адресного пространства сети (во внутренней подсети может использоваться локальная система адресации серверов);
- сокрытие IP-адресов внутренних серверов с целью защиты от хакеров.

Брандмауэры могут работать на разных уровнях протоколов модели **OSI**. *На сетевом уровне* выполняется фильтрация поступающих пакетов, основанная на IP-адресах (например, не пропускать пакеты из Интернета, направленные на те серверы, доступ к которым извне не должен осуществляться; не пропускать пакеты с фальшивыми обратными адресами или с IP-адресами, занесенными в «черный список» и т. д.).
На транспортном уровне фильтрация возможна еще и по номерам портов TCP и флагов, содержащихся в пакетах (например, запросов на установление соединения).
На прикладном уровне может выполняться анализ прикладных протоколов (FTP, HTTP, SMTP и т. д.) и контроль за содержанием потоков данных (запрет внутренним абонентам на получение каких-либо типов файлов: рекламной информации или исполняемых программных модулей, например).
В брандмауэре возможно наличие экспертной системы, которая, анализируя трафик, диагностирует события, потенциально представляющие угрозу безопасности внутренней сети, извещает об этом администратора сети, а в случае опасности она может автоматически ужесточать условия фильтрации и т. д.

Основные компоненты брандмауэра:

- политика сетевого доступа;
- механизмы усиленной аутентификации;
- фильтрация пакетов;
- прикладные шлюзы.

В качестве популярных эффективных брандмауэров называются: ***Netscreen 100, CyberGuard Firewall, Kerio Winroute Firewall, Zone***

Alarm, Agnitum Autpost Firewall, Jetico Personal Firewall, Internet Connection Firewall. Еще одним способом сетевой защиты может быть установленное на сервере специальное программное обеспечение, которое позволяет остальным компьютерам сети эмулировать выход в Интернет, оставаясь при этом «невидимым» со стороны глобальной сети. Такой компьютер называют *прокси-сервером (proxy - доверенный)*. Например, ***Microsoft Proxy Server 2.0.***который, являясь кэширующим сервером (повышает эффективность работы сети – сокращает сетевой трафик), выполняет функции брандмауэра и обеспечивает безопасный доступ в Интернет и имеет два сетевых адаптера – один соединяет его с сетью, другой – с Интернет. Так как локальная сеть «не видна» из Интернет, то легальный IP-адрес имеет только внешний сетевой интерфейс, а IP-адреса внутри сети могут быть выданы из пула, зарезервированного для изолированных сетей.В ОС **Windows XP** с установленным **SP2** (*Service Pack 2* – пакет обновлений 2) входит брандмауэр. Основные возможности: блокировка доступа компьютерным вирусам и червям, запрос пользователя о выборе действия, ведение журнала безопасности.

Выполнение работы

1. Задание 1. Подготовьте компьютер для выполнения лабораторной работы:

1. Запустите виртуальную машину **VM-1.**
2. Перейдите в полноэкранный режим работы

Выполняйте остальные задания лабораторной работы в виртуальной машине.

Задание 2. Создайте новую политику IP-безопасности на локальном компьютере:

1. Откройте оснастку **Управление политикой безопасности IP**:
   - откройте диалоговое окно **Запуск программ (*Пуск/Выполнить*)**;
   - введите команду **mmc** и нажмите клавишу ***ENTER***;
   - выполните команду меню ***Консоль/Добавить или удалить оснастку***;
   - откройте окно с доступными оснастками с помощью кнопки ***Добавить***;
   - выберите в списке элемент *Управление политикой безопасности IP* и добавьте его с помощью кнопки ***Добавить***;
   - завершите добавление оснастки кнопкой ***Готово***;
   - закройте диалоговое окно **Добавить изолированную оснастку**;
   - закройте диалоговое окно **Добавить/Удалить оснастку** с помощью кнопки ***OK***.
2. Активизируйте оснастку **Политика безопасности IP на «Локальный компьютер»**.

Справа отобразятся установленные по умолчанию политики.

3. Запустите мастер создания политик безопасности:
   - вызовите контекстное меню оснастки **Политика безопасности IP на «Локальный компьютер»**
   - выполните команду **Создать политику безопасности IP…**.

4. Ознакомьтесь с информацией мастера и щелкните по кнопке ***Далее***.

5. Установите *Имя политики безопасности IP*:

- введите в поле **Имя** – *My_politic*.
- введите в поле **Описание** – *Это политика IP безопасности локального компьютера* и щелкните по кнопке ***Далее***.

6. Настройте *политику безопасного соединения*. Для этого установите флажок *Использовать правило по умолчанию* и щелкните по кнопке ***Далее***.

7. Установите *Способ проверки подлинности правила отклика по умолчанию*:

- активизируйте **Использовать данную строку для защиты обмена ключами**;
- введите в нижнее поле *123456789*;
- закройте окно кнопкой ***Далее***.

8. Закройте мастера создания политики безопасности кнопкой ***Готово***. *Откроется диалоговое окно* ***Свойства: My_politic***.

9.

10. Запустите **Мастер правил безопасности** и настройте правила безопасности:

- запустите мастер кнопкой ***Добавить***;
- ознакомьтесь с описанием мастера и - ***Далее***;
- выберите *Это правило не определяет туннель* и щелкните ***Далее***;
- выберите *Локальные сетевые подключения* и щелкните ***Далее***;
- выберите *Использовать сертификат данного центра сертификации (ЦС)*;
- щелкните **Обзор** и выберите любой сертификат, кнопка ***Далее***;
- в списке фильтров IP выберите *Полный IP трафик* и щелкните ***Далее***;
- добавьте *новое действие фильтра*:
  - щелкните по кнопке ***Добавить***;
  - ознакомьтесь с описанием запустившегося мастера и - ***Далее***;
  - введите в поле **Имя** – *My_filter* и щелкните по кнопке ***Далее***;
  - выберите *Разрешить* и щелкните по кнопке ***Далее***;
  - завершите добавление нового действия кнопкой ***Готово***.
- активизируйте созданное вами действие и измените его параметры:
  - щелкните по кнопке ***Изменить***;
  - выберите *Согласовать безопасность*;
  - щелкните по кнопке ***Добавить*** и выберите *Шифрование и обеспечение целостности*;
  - установите флажок *Принимать небезопасную связь, но отвечать с помощью IPSEC* и щелкните по кнопке ***Далее***;
- завершите работу мастер кнопкой ***Готово***.

11. Добавьте в политику фильтр для блокировки всех входящих подключений:

- отключите использование мастера (флажок *Использовать мастер*);

- откройте диалоговое окно **Созданий новых правил** кнопкой ***Добавить***;
- откройте диалоговое окно **Добавление фильтра** кнопкой ***Добавить***;
- добавьте новый фильтр:
  - сбросьте флажок *Использовать мастер*;
  - откройте диалоговое окно **Свойства: Фильтр** кнопкой ***Добавить***;
  - в поле **Адрес источника пакетов** выберите *Любой адрес IP*;
  - в поле **Адрес назначения пакетов** выберите *Мой IP адрес*;
  - установите флажок *Отраженный для блокировки приходящих пакетов*;
  - установите *протокол TCP* для фильтрации (***вкладка Протокол\раскрывающийся список Выберите протокол***);
  - завершите настройку нового фильтра кнопкой ***ОК***;
- закройте диалоговое окно **Список фильтров** кнопкой ***ОК***.
- завершите добавление нового правила кнопкой ***ОК***.

12. Закройте диалоговое окно **Свойства: My_politic**.
13. Активизируйте выбранную политику (***контекстное меню созданной политики/Назначить***).
14. Проверьте работу политики, воспользовавшись утилитой **ping** на другом компьютере.

*Если политика настроена верно, то утилита **ping** выдаст сведения о том что данный компьютер недоступен.*

Задание 3.Настройте фильтрацию IP -трафика.

1. Откройте диалоговое окно свойств **Подключения по локальной сети (*Пуск/Панель управления/Сетевые подключения*)**.
2. Откройте диалоговое окно **Свойства: Протокол Интернета (TCP/IP)** и щелкните по кнопке ***Дополнительно***.
3. Перейдите на вкладку **Параметры**.
4. Откройте окно **Фильтрация TCP/IP** с помощью кнопки ***Свойства***.
5. Установите TCP-порты, которые можно использовать:
   - выберите в разделе **TCP-порты** переключатель *Только* и щелкните по кнопке ***Добавить***;
   - введите **номер порта для протокола HTTPS** – *443*;
   - аналогично добавьте порты
     - для **протокола отправки почты SMTP** – *25*;
     - для **протокола получения почты POP3** – *110*;
     - **протокол FTP** – *21*;
     - **протокол Telnet** - *23*.
   - Щелкните ***ОК*** для применения параметров.
6. Запретите использование протокола **Telnet**.
7. Закройте окно **Дополнительные параметры TCP/IP** кнопкой ***ОК***.
8. Закройте окно **Свойства: Протокол Интернета (TCP/IP)** кнопкой ***ОК***.

9. Проверьте настроенную фильтрацию. Для этого подключитесь по протоколу **Telnet** с другого компьютера (*программа **Telnet** входит в состав ОС **Windows** и используется для работы на удаленном компьютере в командной строке*).

Задание 4. Настройте брандмауэр Windows:

1. Откройте **настройки брандмауэра (*Пуск/Панель управления/Центр обеспечения безопасности/Брандмауэр Windows*)**.
2. Разрешите доступ браузеру **Internet Explorer** к Интернету:
   - перейдите на вкладку **Исключения** и щелкните по кнопке ***Добавить программу***.
   - выберите в списке **Internet Explorer** и щелкните по кнопке ***ОК***.
3. Включите ведение журнала безопасности:
   - перейдите на вкладку **Дополнительно**;
   - щелкните по кнопке ***Параметры*** в разделе **Ведение журнала безопасности**;
   - включите запись пропущенных и успешных пакетов;
   - сохраните сделанные изменения кнопкой ***ОК***.
4. Завершите конфигурирование брандмауэра кнопкой ***ОК***.
5. Подключитесь к сети Интернет с помощью браузера **Internet Explorer**

Если все настроено правильно, то вы сможете выйти в Интернет, в противном случае брандмауэр выдаст сообщение о том, что какая-то программа пытается получить доступ в Интернет.

Лабораторная работа 9. Создание резервных копий

Цель: научиться выполнять архивирование данных и пользоваться службой восстановления системы.

Средства для выполнения работы:

• аппаратные: компьютер с установленной ОС Windows XP.

• программные: приложения ВМ: VirtualBox; виртуальные машины: VM-1.

Теоретические сведения

Архивация и восстановление

Мастер архивации и восстановления (*Backup or Restore Wizard*) создает копию файлов и папок на указанном пользователем носителе информации. В случае потери или повреждения пользовательских данных их можно восстановить из файла резервной копии. Специалисты рекомендуют выполнять регулярное создание резервных копий важных файлов и папок. Частота архивации (*резервного копирования*) зависит от частоты изменений файлов, так как в случае потери данных придется повторно создать то, что было сделано после последней архивации. По этой причине многие компании создают резервные копии важных файлов ежедневно. Пользователь может выбирать различные типы архивации в зависимости от его требований.

• Для типа *Обычная (**Normal**)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, и каждый файл маркируется как прошедший архивацию (имеющий резервную копию).

• Для типа *Копирование (**Copy**)* происходит архивация всех выбранных файлов и системных настроек для определенной папки или диска, но файлы не маркируются как прошедшие архивацию.

• Для типа *Добавочная (**Incremental**)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, и каждый файл маркируется как прошедший архивацию.

• Для типа *Разностная (**Differential**)* происходит архивация только тех файлов, которые были созданы или изменены вслед за последней обычной или добавочной архивацией, но файлы не маркируются.

• Для типа *Ежедневная (**Daily**)* происходит архивация только тех файлов, которые были созданы или изменены в данный день, но файлы не маркируются.

Тип архивации, который применяется, определяет, насколько сложным будет процесс восстановления. Для восстановления после нескольких добавочных или разностных архиваций необходимо выполнить восстановление из последней обычной резервной копии и из всех добавочных или разностных копий, полученных после обычной архивации и вплоть до настоящего момента.

Выполняя архивацию данных, пользователь указываете имя и место для файла резервной копии. По умолчанию файлы резервных копий сохраняются с расширением ***.bkf***. Файлы архивации можно сохранять на жестком диске, на гибком диске или на любом другом типе съемного носителя. При выборе места для резервной копии нужно учитывать размер файла архивации, типы имеющихся носителей, а также возможное требование того, что файлы

резервных копий нужно хранить отдельно от компьютера на случай катастрофы.

Функция восстановления системы

Восстановление системы позволяет выполнить откат состояния операционной системы к одной из точек восстановления, фиксирующих состояние на момент, когда система стабильно работала. Преимуществом данной функции заключается в том, что она предоставляет возможность быстрого восстановления ("отката" состояния системы к с остоянию, в котором она находилась в один из предыдущих моментов во времени) без переустановки системы, а также не подвергает риску случайного перезаписывания рабочих файлов пользователей. Возможно выполнение отката к любому из следующих типов контрольных точек и точек восстановления.

• *Начальная контрольная точка (**initial system checkpoint**)* системы создается при первом запуске компьютера с вновь установленной ОС.

• Точки восстановления *для автоматических обновлений (**Automatic update restore points**)* создаются, когда инсталлируются обновления, которые загружаются с помощью **Windows Update**.

• Точки восстановления *при восстановлении с резервной копии (**Backup recovery restore points**)* создаются, когда пользователь использует мастер архивации или восстановления (**Backup or Restore Wizard**).

• Пользователь может создавать свои *собственные точки восстановления вручную (**"ручные" контрольные точки - manual checkpoints**)* в любой момент с помощью мастера восстановления системы (**System Restore Wizard**).

• Точки восстановления *при инсталляции программ (**Program name installation restore points**)* создаются, при установке программного обеспечения.

• Точки восстановления *для операции восстановления (**Restore operation restore points**)* создаются каждый раз, когда пользователь осуществляете какое-либо восстановление.

• *Системные контрольные точки (**System checkpoints**)* - это запланированные точки восстановления, которые создаются компьютером регулярно, даже если пользователь не вносил никаких изменений в систему.

• Точки восстановления *для неопознанного устройства (**Unsigned device driver restore points**)* создаются, когда устанавливается драйвер устройства, который не был опознан или сертифицирован.

Средство **Восстановление системы (*System Restore*)** обычно сохраняет набор контрольных точек восстановления за период от одной до трех недель. Количество контрольных точек восстановления, доступных в любой заданный момент времени, ограничено объемом пространства, которое выделено пользователем для работы системы восстановления. Максимальный размер пространства, которое можно выделить, составляет приблизительно 12 процентов.

В ходе процедуры восстановления происходит восстановление ОС и программ, инсталлированных на компьютере, к состоянию, в котором они находились на момент выбранной контрольной точки восстановления. Этот процесс не затрагивает личные файлы пользователя (включая сохраненные

документы, сообщения электронной почты, адресную книгу, список **Избранные (*Favorites*)** и список**Журнал (*History*) Интернет Explorer**).

Все изменения, внесенные утилитой **Восстановление системы (*System Restore*)**, полностью обратимы, и если пользователя не удовлетворяют результаты, то можно восстановить предыдущие настройки и выполнить все снова.

Выполнение работы

Задание 1. Выполните резервное копирование системных конфигурационных файлов.

1. Запустите виртуальную машину **VM-1** и загрузите ОС **Windows**.
2. Запустите **Мастер Архивации (*Пуск/Программы/Стандартные/Служебные/Архивация данных*)**.
3. ознакомьтесь с информацией мастера и щелкните ***Далее***.

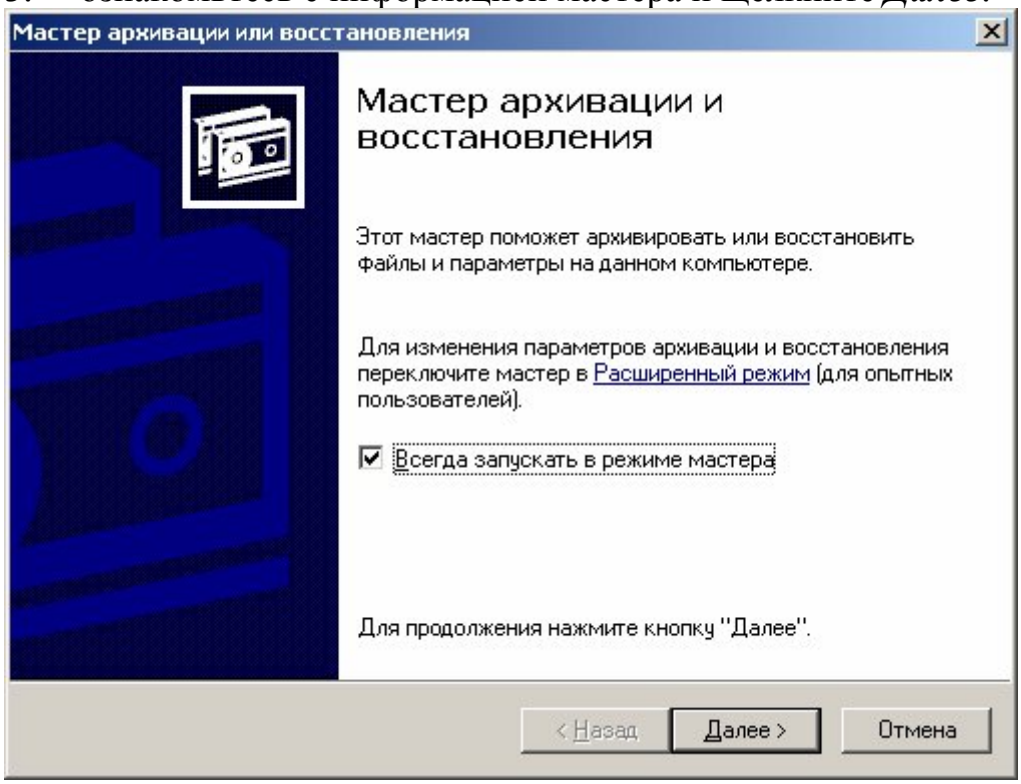

Рисунок 1. Мастер Архивации данных.

4. Выберите возможность мастера – **Архивация файлов и параметров** и щелкните ***Далее***.

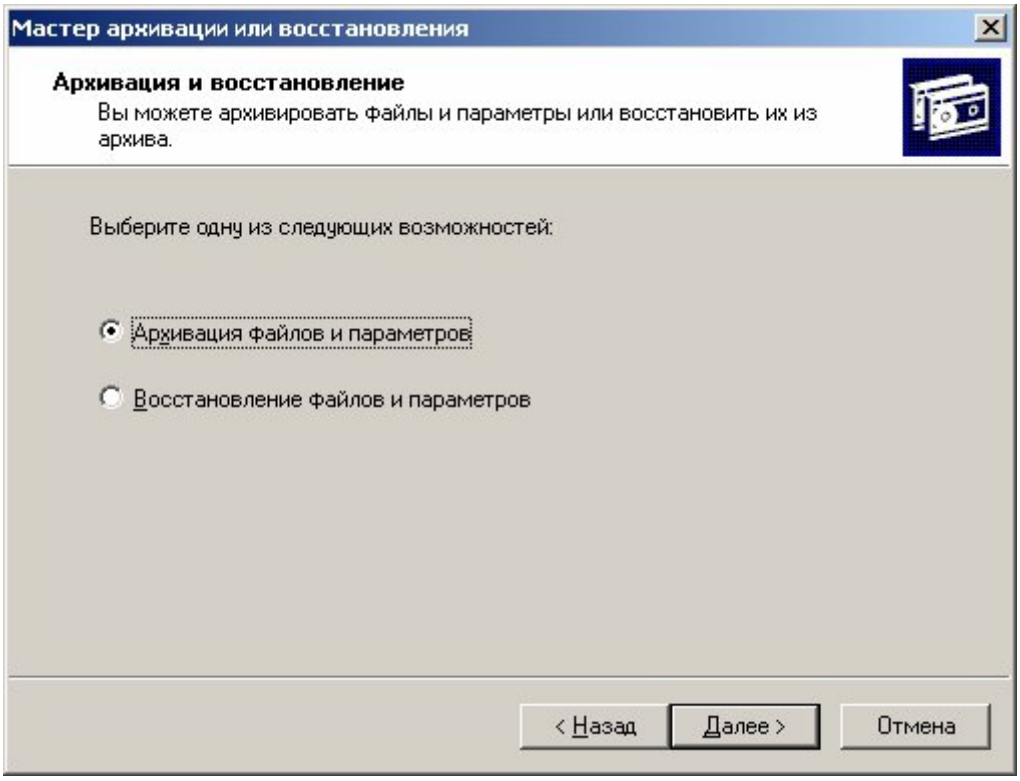

Рисунок 2. Выбор архивации или восстановления.

5. Укажите выбор элементов архивирования в самостоятельном режиме – *Предоставить возможность выбора объектов для архивации* и щелкните ***Далее***.

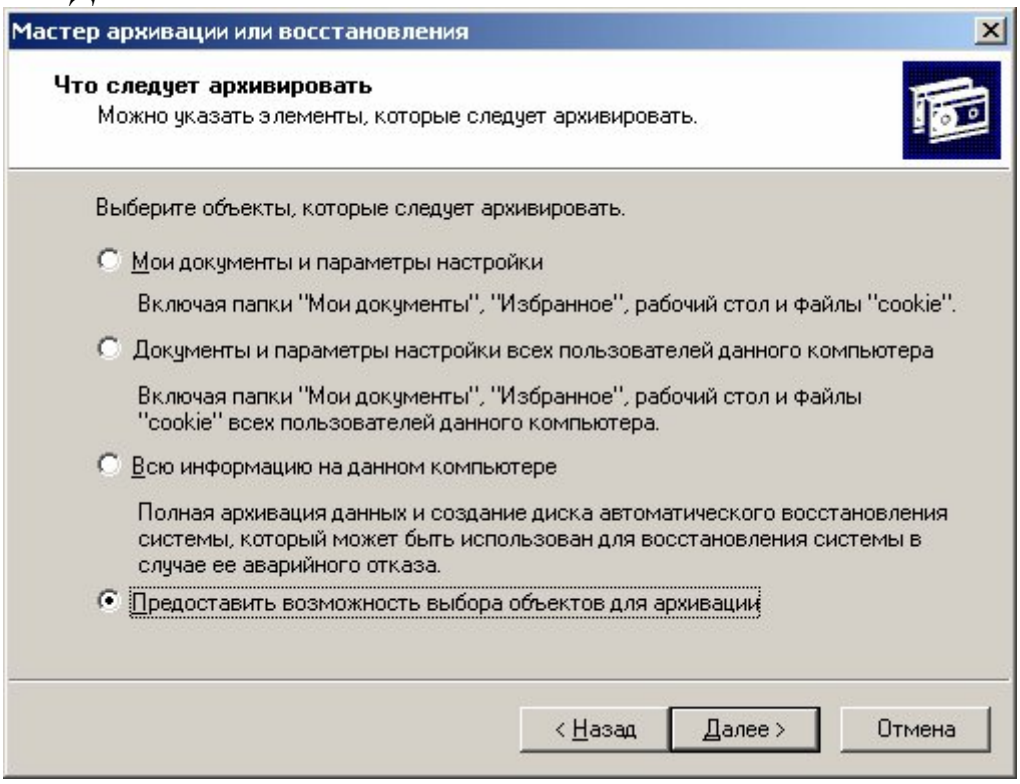

Рисунок 3. Выбор способа указаний объектов архивирования.

6. Укажите элементы для архивации – папки ***Documents and Settings*** и ***Program Files*** и щелкните ***Далее***.

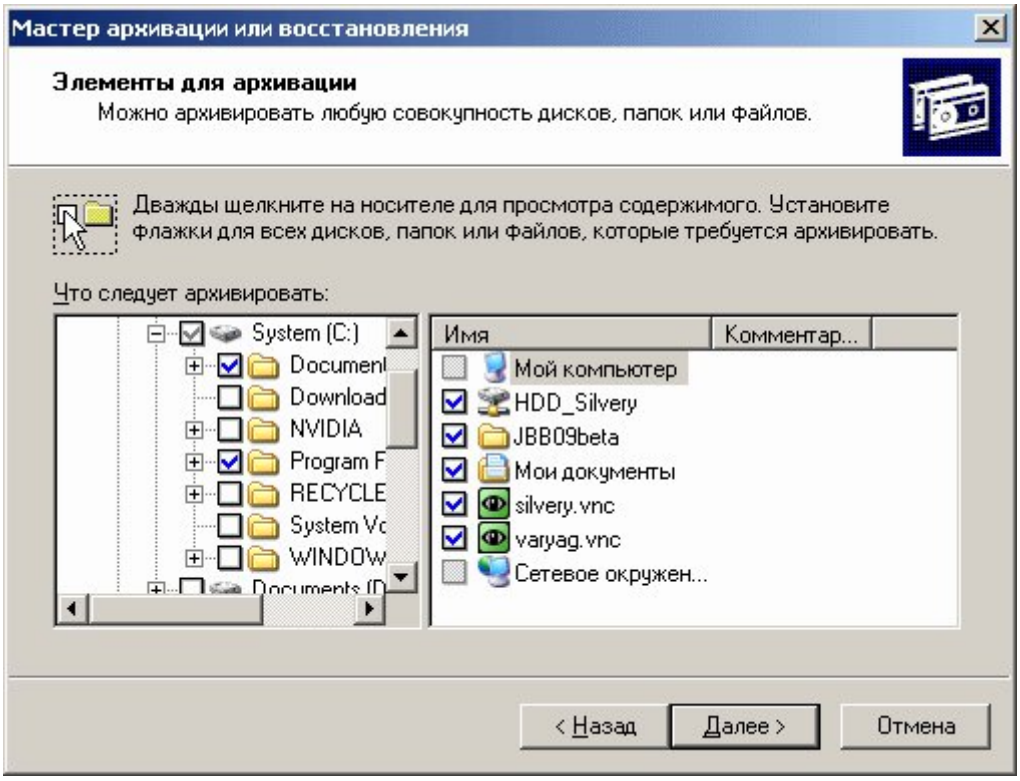

Рисунок 4. Выбор объектов архивирования.

7. Укажите место хранения архива:
   - откройте диалоговое окно **Сохранить** как кнопкой ***Обзор***;

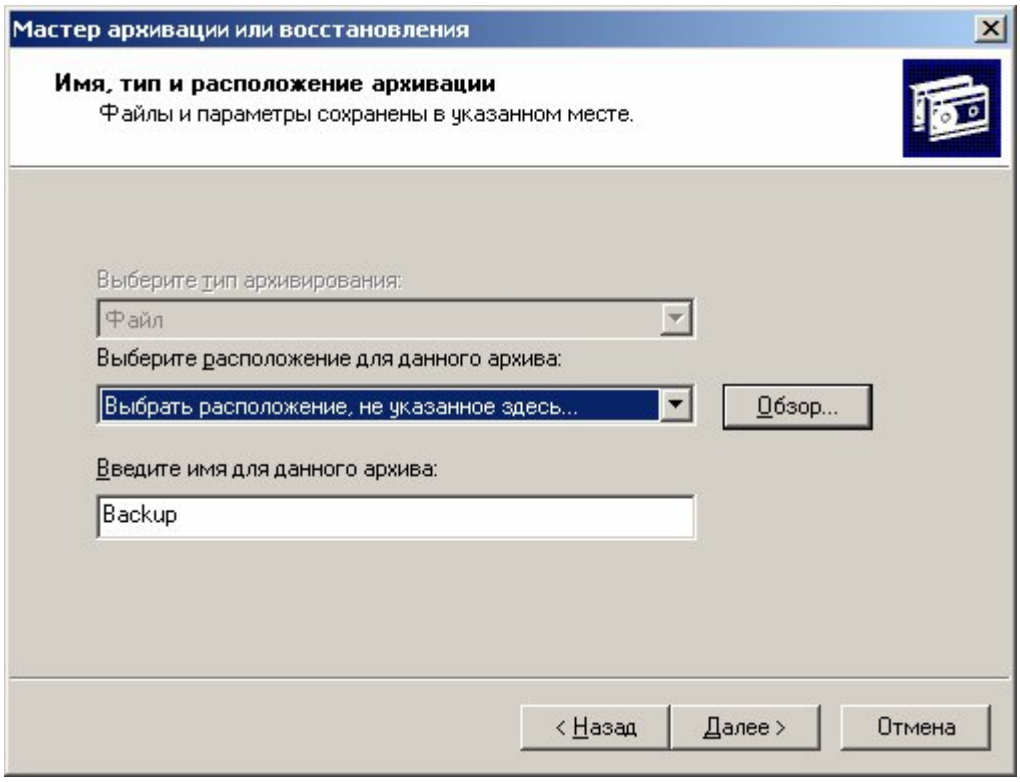

Рисунок 5. Выбор места хранеиня архива.

   - перейдите в корневой каталог диска **C**;
   - введите в поле **Имя Файла** – имя сохраняемого файла - *Резервная Копия*;
   - сохраните файл кнопкой ***Сохранить***;

- подтвердите введенные данные кнопкой ***Далее***.

8. Настройте дополнительные параметры архивации:

- откройте диалоговое окно дополнительных параметров кнопкой ***Дополнительно***;
- выберите в раскрывающемся списке **тип архивации** – *Обычный* и щелкните ***Далее***;
- установите флажок *Проверять данные после архивации* (***Далее***);
- укажите **способ добавления архива** – *Добавить этот архив к существующему* (***Далее***);
- укажите **время архивации**:
  - установите радиокнопку *Позднее*;
  - введите имя задания в соответствующее поле;

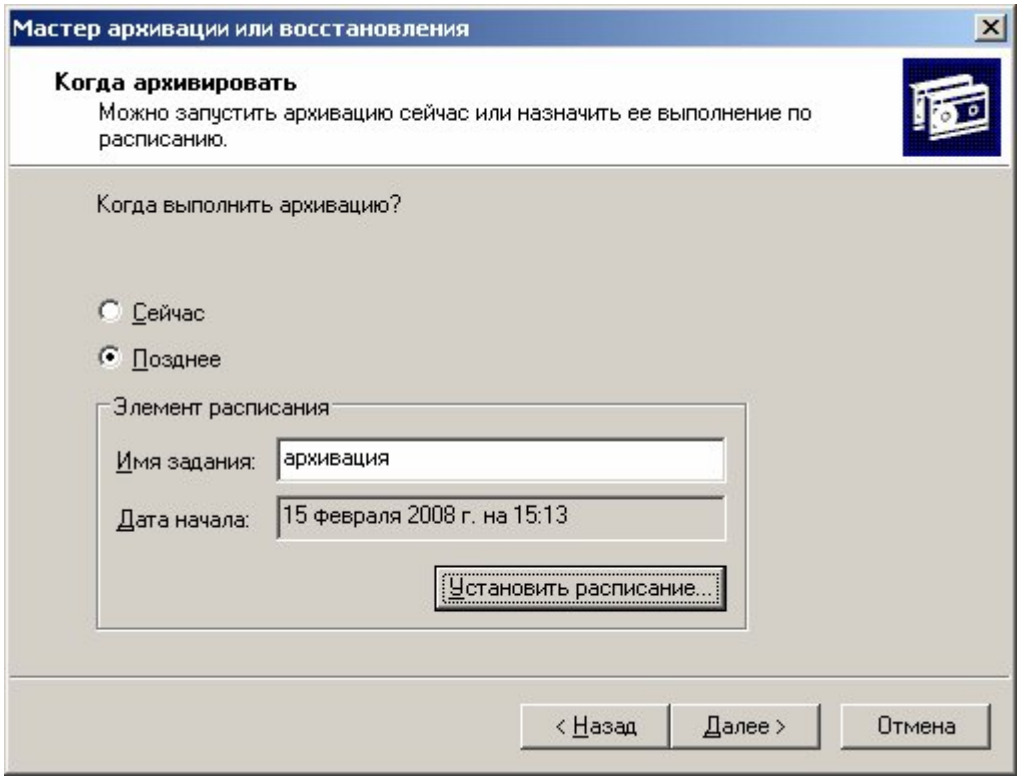

Рисунок 6. Указание имени и времени выполнения архивирования.

- откройте диалоговое окно **Запланированное задание** кнопкой ***Расписание***;

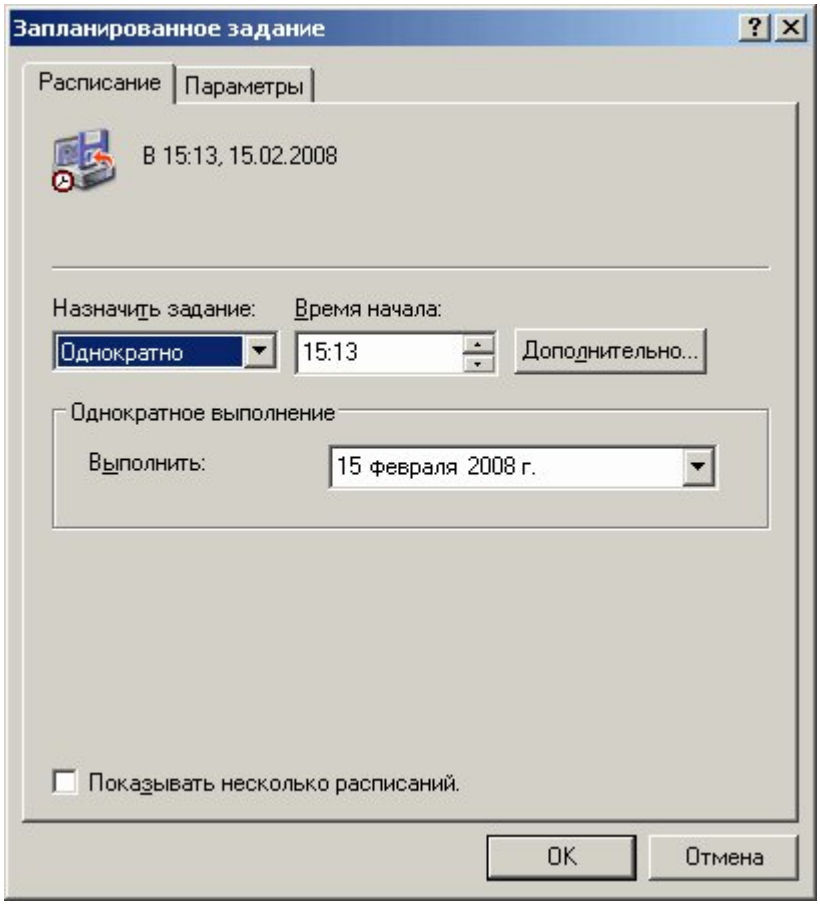

Рисунок 7. Указание точного времени начала выполнения архивирования.

- введите в поле **Время начала** время на *2* минуты позже текущего (например, если сейчас 12.40, то вам необходимо ввести 12.42);
- подтвердите введенные параметры кнопкой ***ОК***;
- завершите ввод времени выполнения архивации кнопкой ***Далее***;
- введите данные пользователя от имени которого будет выполняться архивирование:
  - введите в поле **Пользователь** имя пользователя на компьютере - *USER*;
  - введите в поля **Пароль** и **Подтверждение пароля** для пользователя *USER*;
  - подтвердите ввод данных кнопкой ***ОК***;

9. завершите работу мастера кнопкой ***Готово***.

Задание 2. Выполните восстановление системных конфигурационных файлов.

1. Запустите **Мастер Архивации (*Пуск/Программы/Стандартные/Служебные/Архивация данных*)**.
2. Ознакомьтесь с информацией мастера и щелкните ***Далее***.
3. Выберите возможность мастера – **Восстановление файлов и параметров** и щелкните ***Далее***.
4. Выберите для восстановления в левом списке с содержимым архива, папку ***Мои рисунки*** (***Далее***);.

5. Ознакомьтесь с выбранными параметрами и активизируйте восстановление кнопкой ***Готово***.

6. Откройте отчет кнопкой ***Отчет*** и просмотрите его.

7. Закройте диалоговое окно **Ход восстановления** кнопкой ***Закрыть***.

Задание 3. Создайте точку восстановления.

1. Запустите мастер **Восстановление системы (*Пуск/Программы/Стандартные/Служебные*)**.

2. Ознакомьтесь с информацией мастера.

3. Создайте точку восстановления:

- Установите радиокнопку *Создать точку восстановления* (***Далее***);
- введите в текстовое поле **Описание контрольной точки восстановления** - *Тестовая точка восстановления*;

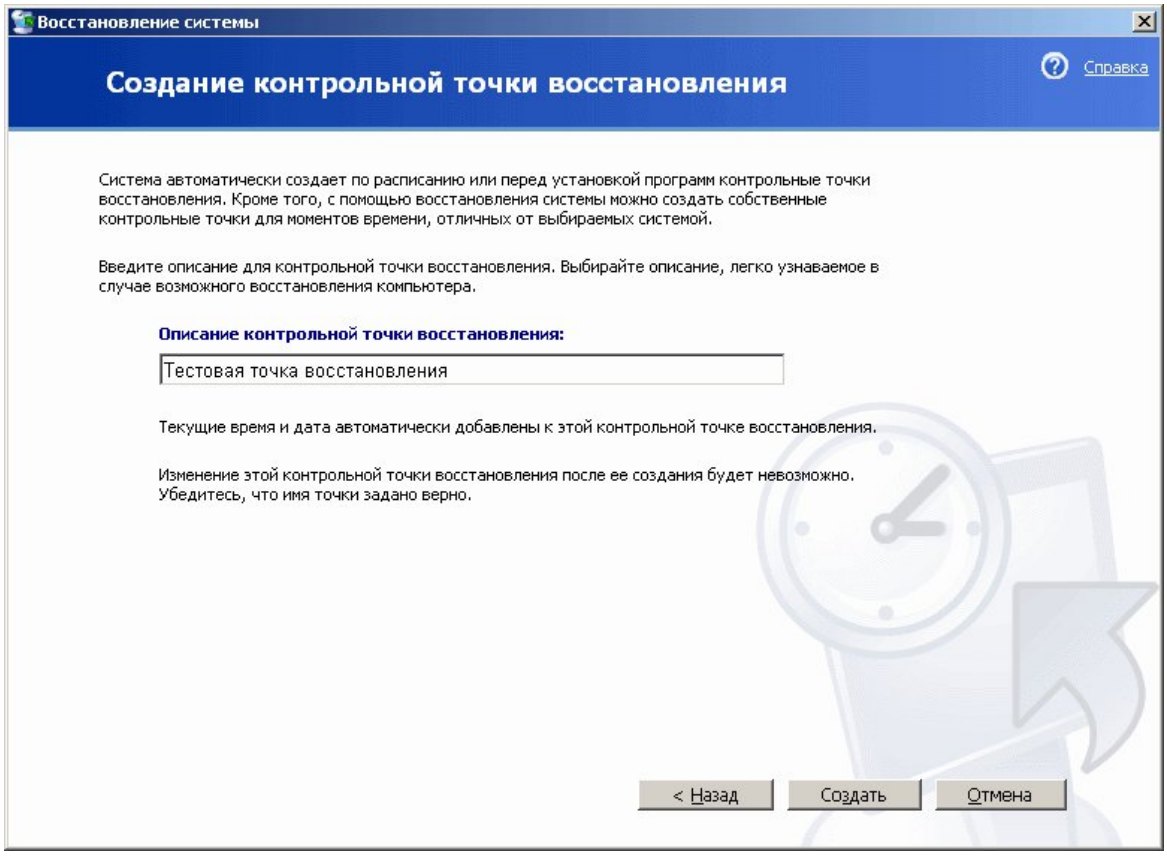

Рисунок 8. Восстановление системы.

- создайте точку восстановления кнопкой ***Создать***.

4. Завершите работу мастера кнопкой ***Закрыть***

Лабораторная работа 10. Создание баз данных (БД) в Microsoft SQL Server

Цель работы – с помощью операторов языка Transact SQL научиться создавать базы данных и совокупность связанных таблиц, принадлежащих указанной базе данных.

Содержание работы:

1. Познакомиться с набором утилит, входящих в состав MS SQL Server 2008.
2. Познакомиться с работой утилит SQL Server Enterprise MANAGER и Query Analyzer.
3. Создать с помощью приведенных операторов пример базы данных «Книжное дело».
4. По выданным вариантам создать персональную базу данных с набором связанных таблиц.

Пояснения к выполнению работы

В качестве примера базы данных, которая будет создана программно с помощью операторов языка Transact SQL, выберем БД «Книжное дело» (рис. 1.1). Структура таблиц данной БД представлена в табл. 1.1-1.5.

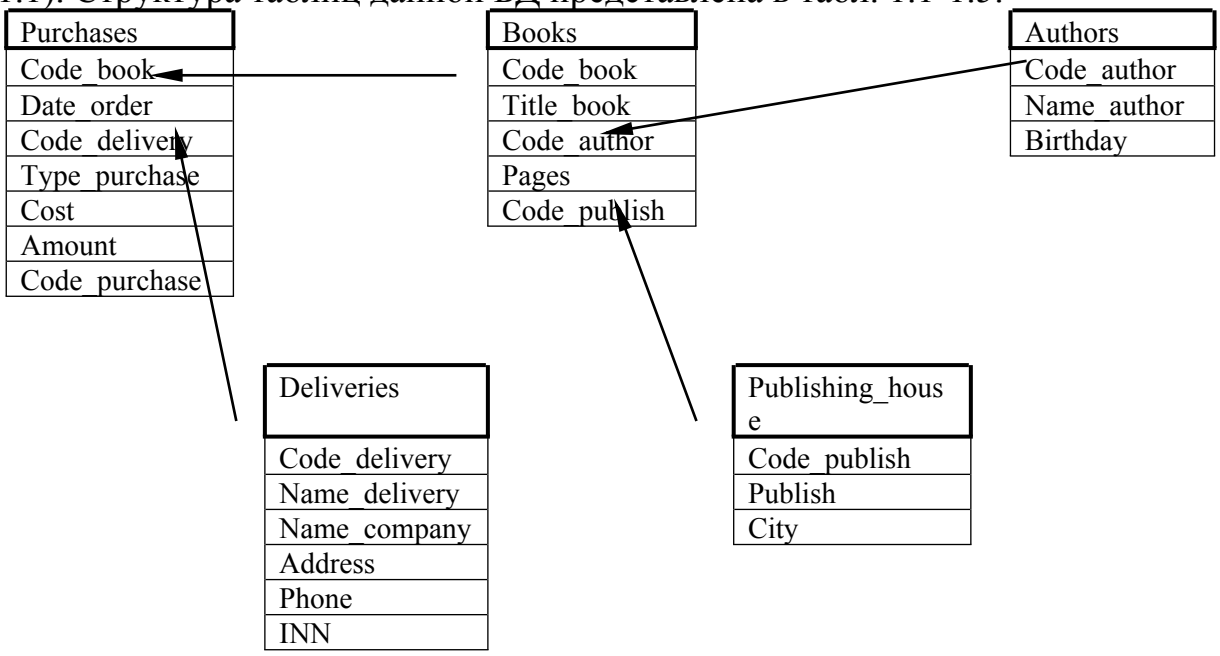

Рис. 1.1. Фрагмент базы данных «Книжное дело»

Таблица 1.1

Покупки (название таблицы Purchases)

Название поля	Тип поля	Описание поля
Code_book	Int	Код закупаемой книги
Date_order	DateTime	Дата заказа книги
Code_delivery	Int	Код поставщика
Type_purchase	Bit	Тип закупки (опт/ розница)
Cost	Money	Стоимость единицы товара
Amount	Int	Количество экземпляров
Code_purchase	Int	Код покупки

Таблица 1.2

Справочник книг (название таблицы Books)

Название поля	Тип поля	Описание поля
Code_book	Int	Код книги
Title_book	Char	Название книги
Code_author	Int	Код автора
Pages	Int	Количество страниц
Code_publish	Int	Код издательства

Таблица 1.3

Справочник авторов (название таблицы Authors)

Название поля	Тип поля	Описание поля
Code_author	Int	Код автора
Name_author	Char	Фамилия, имя, отчество автора
Birthday	DateTime	Дата рождения

Таблица 1.4

Справочник поставщиков (название таблицы Deliveries)

Название поля	Тип поля	Описание поля
Code_delivery	Int	Код поставщика
Name_delivery	Char	Фамилия, и., о. ответственного лица
Name_company	Char	Название компании-поставщика
Address	Char	Юридический адрес
Phone	Numeric	Телефон контактный
INN	Char	ИНН

Таблица 1.5

Справочник издательств (название таблицы Publishing_house)

Название поля	Тип поля	Описание поля
Code_publish	Int	Код издательства
Publish	Char	Издательство
City	Char	Город

Запустить **SSQL Server Management Studio,** проверить включение сервера.

Создать новую базу данных с названием **DB_Books** в утилите «Создать запрос» («New query») с помощью команды:

CREATE DATABASE DB_BOOKS

Для выполнения команды нажать F5.

Открыть утилиту **SQL Server Management Studio.** Проверить наличие БД DB_Books, если ее не видите в разделе DataBases, то нажмите F5 для обновления.

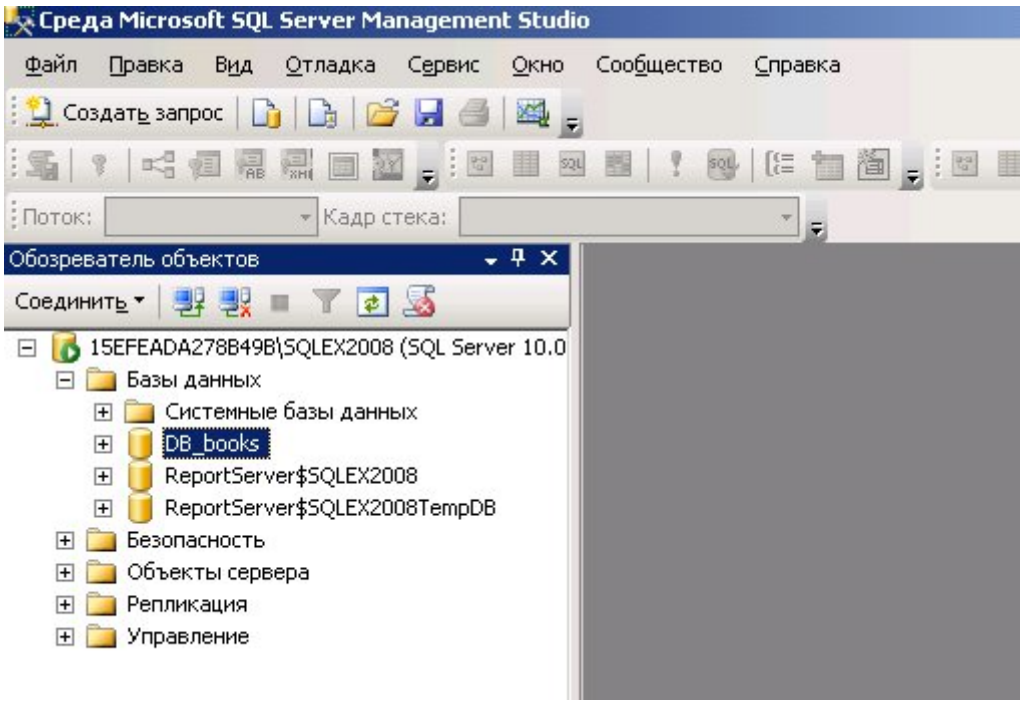

Рис. 1.2. Результат создания БД

Создать в ней перечисленные таблицы либо с помощью мастера таблиц, либо через «Создать запрос» с помощью следующих команд:

use DB_BOOKS

CREATE TABLE Authors(Code_author INT PRIMARY KEY, name_author CHAR(30), Birthday DATETIME)

CREATE TABLE Publishing_house(Code_publish INT PRIMARY KEY, Publish CHAR(30), City CHAR(20))

CREATE TABLE Books(Code_book INT PRIMARY KEY, Title_book CHAR(40), Code_author INT FOREIGN KEY REFERENCES Authors(Code_author), Pages INT, Code_publish INT FOREIGN KEY REFERENCES Publishing_house(Code_publish))

CREATE TABLE Deliveries(Code_delivery INT PRIMARY KEY, Name_delivery CHAR(30), Name_company CHAR(20), Address VARCHAR(100), Phone BIGINT, INN CHAR(13))

CREATE TABLE Purchases(Code_purchase INT PRIMARY KEY, Code_book INT FOREIGN KEY REFERENCES Books(Code_book), Date_order SMALLDATETIME, Code_delivery INT FOREIGN KEY REFERENCES Deliveries(Code_delivery), Type_purchase BIT, Cost FLOAT, Amount INT)

Открыть утилиту SQL Server Enterprise MANAGER. Проверить наличие БД DB_Books.

В разделе диаграмм создать новую диаграмму, в которую добавить из списка пять наших таблиц, проверить связи между таблицами.

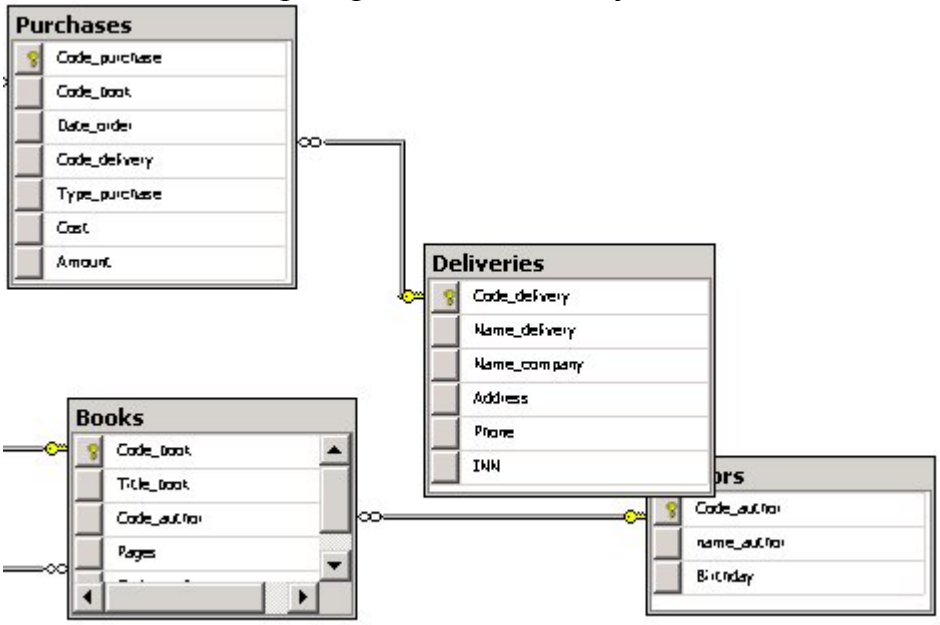

Рис. 1.3. Результат создание диаграммы

Использованные операторы:

PRIMARY KEY – признак создания ключевого поля.

FOREIGN KEY**...**REFERENCES… – признак создания поля связи с другой таблицей.

CREATE TABLE – команда создания таблицы в текущей БД.

USE – сделать активной конкретную БД.

CREATE DATABASE – команда создания новой БД.

Варианты заданий к лабораторной работе №1

Общие положения

В утилите «Создать запрос» создать новую базу данных с помощью оператора **Create Database**, название БД определить, исходя из предметной области. Закомментировать оператор (-- – однострочный комментарий, /* */ – многострочный комментарий). Программно сделать активной созданную БД с помощью оператора **Use**. Создать перечисленные таблицы с помощью операторов **Create table**, причем самостоятельно определить типы таблиц (родительская или подчиненная), типы полей и их размеры, найти поля типа Primary key и Foreign key. Сохранить файл программы с названием **ФамилияСтудента_ЛАб_1_№варианта.** В SQL Server Enterprise MANAGER в разделе диаграмм созданной БД сгенерировать новую диаграмму, проверить связи между таблицами.

Вариант 1. БД «Учет выданных подарков несовершеннолетним детям сотрудников предприятия»

Код сотрудника
Фамилия
Имя
Отчество
Должность
Подразделение
Дата приема на работу

Код сотрудника
Имя ребенка
Дата рождения
Код ребенка

Код ребенка
Стоимость подарка
Дата выдачи подарка
Код выдачи

Вариант 2. БД «Учет выполненных ремонтных работ»

Код прибора в ремонте
Название прибора
Тип прибора
Дата производства

Код прибора
Код мастера
ФИО владельца прибора
Дата приема в ремонт
Вид поломки
Стоимость ремонта
Код ремонта

Код мастера
Фамилия мастера
Имя мастера
Отчество мастера
Разряд мастера
Дата приема на работу

Вариант 3. БД «Продажа цветов»

Код цветка
Название цветка
Сорт цветка
Средняя высота
Тип листа
Цветущий
Дополнительные сведения

Код цветка
Дата продажи
Цена продажи
Код продавца
Код продажи

Код продавца
Фамилия
Имя
Отчество
Разряд
Оклад
Дата приема на работу

Вариант 4. БД «Поступление лекарственных средств»

Код лекарства
Название лекарства
Показания к применению
Единица измерения
Количество в упаковке
Название

Код лекарства
Код поставщика
Дата поставки
Цена за единицу
Количество
Код

Код поставщика
Сокращенное название
Полное название
Юридический адрес
Телефон
ФИО руководителя

производителя	поступления	

Вариант 5. БД «Списание оборудования»

Код оборудования	Код оборудования	Код сотрудника
Название оборудования	Причина списания	Фамилия
Тип оборудования	Дата списания	Имя
Дата поступления	Код сотрудника	Отчество
ФИО ответственного	Код списания	Должность
Место установки		Подразделение
		Дата приема на работу

Вариант 6. БД «Поваренная книга»

Код блюда	Код блюда	Код продукта
Тип блюда	Код продукта	Название продукта
Вес блюда	Объем продукта	Ед измерения
Порядок приготовления		
Количество калорий		
Количество углеводов		

Вариант 7. БД «Регистрация входящей документации»

Код регистратора	Код документа	Код организации-отправителя
Фамилия	Номер документа	Сокращенное название
Имя	Дата регистрации	Полное название
Отчество	Краткое содержание документа	Юридический адрес
Должность	Тип документа	Телефон
Дата приема на работу	Код организации-отправителя	ФИО руководителя
	Код регистратора	

Вариант 9. БД «Увольнение сотрудника»

Код сотрудника	Код документа	Код статьи увольнения
Фамилия	Номер документа	Название статьи увольнения
Имя	Дата регистрации	Причина увольнения
Отчество	Дата увольнения	Номер статьи увольнения
Должность	Код статьи увольнения	Номер пункта/ подпункта увольнения

Подразделение	Код сотрудника	
Дата приема на работу	Денежная компенсация	

Вариант 9. БД «Приказ на отпуск»

Код сотрудника	Код документа	Код отпуска
Фамилия	Номер документа	Тип отпуска
Имя	Дата регистрации	Оплата отпуска
Отчество	Дата начала отпуска	Льготы по опуску
Должность	Дата окончания отпуска	
Подразделение	Код сотрудника	
Дата приема на работу	Код отпуска	

Вариант 10. БД «Регистрация выходящей документации»

Код отправителя	Код документа	Код организации-получателя
Фамилия	Номер документа	Сокращенное название
Имя	Дата регистрации	Полное название
Отчество	Краткое содержание документа	Юридический адрес
Должность	Тип документа	Телефон
Дата приема на работу	Код организации-получателя	ФИО руководителя
	Код отправителя	

Вариант 11. БД «Назначение на должность»

Код сотрудника	Код документа	Код должности
Фамилия	Номер документа	Название должности
Имя	Дата регистрации	Льготы по должности
Отчество	Дата назначения	Требования к квалификации
Дата приема на работу	Код сотрудника	
Дата рождения	Код должности	
Пол		

Вариант 12. БД «Выдача оборудования в прокат»

Код клиента	Код выдачи	Код оборудования
Фамилия	Номер документа	Название оборудования
Имя	Дата начала проката	Тип оборудования
Отчество	Дата окончания проката	Дата поступления в прокат

Адрес
Телефон
Серия и номер паспорта

Код оборудования
Код клиента
Стоимость

Вариант 13. БД «Списание оборудования из проката»

Код оборудования
Название оборудования
Тип оборудования
Дата поступления в прокат

Код оборудования
Причина списания
Дата списания
Код сотрудника
Номер документа
Дата регистрации
Код списания

Код сотрудника
Фамилия
Имя
Отчество
Должность
Дата приема на работу

Вариант 14. БД «Прием цветов в магазин»

Код цветка
Название цветка
Сорт цветка
Средняя высота
Тип листа
Цветущий
Дополнительные сведения

Код цветка
Дата поступления
Цена за единицу
Код поставщика
Код поступления
Количество

Код поставщика
Сокращенное название
Полное название
Юридический адрес
Телефон
ФИО руководителя

Вариант 15. БД «Регистрация клиентов гостиницы»

Код номера
Тип номера
Перечень удобств
Цена за сутки

Код регистрации
Код номера
Дата заезда
Дата выезда
Стоимость
Код клиента

Код клиента
Фамилия
Имя
Отчество
Адрес
Телефон
Серия и номер паспорта

Вариант 16. БД «Возврат оборудования в службу проката»

Код клиента
Фамилия
Имя
Отчество
Адрес
Телефон
Серия и номер паспорта

Код возврата
Номер документа
Дата возврата
Состояние оборудования
Код оборудования
Код клиента
Штраф

Код оборудования
Название оборудования
Тип оборудования
Дата поступления в прокат

Вариант 17. БД «Учет материальных ценностей на предприятии»

Код ценности
Название ценности
Тип ценности
Закупочная стоимость
Срок гарантии
Дата начала гарантии

Код постановки на учет
Код ценности
Код материально ответственного
Дата постановки на учет
Место нахождения ценности

Код материально ответственного
Фамилия
Имя
Отчество
Должность
Дата приема на работу
Подразделение

Вариант 18. БД «Состав ремонтных работ»

Код ремонтной работы
Код этапа работы
Название этапа работы
Стоимость этапа

Код ремонтной работы
Код мастера
Стоимость ремонта
Количество дней ремонта
Название ремонтной работы

Код мастера
Фамилия мастера
Имя мастера
Отчество мастера
Разряд мастера
Дата приема на работу

Вариант 19. БД «Продажа лекарственных средств»

Код лекарства
Название лекарства
Показания к применению
Единица измерения
Количество в упаковке

Номер чека
Цена за единицу
Количество
Код лекарства
Код записи в чеках

Номер чека
Дата продажи
Сумма
ФИО кассира

Название производителя		

Вариант 20. БД «Учет исполнения по входящей документации»

Код исполнителя	Код документа	Код документа
Фамилия	Дата назначения на исполнения	Номер документа
Имя	Срок выполнения в днях	Дата регистрации
Отчество	Тип результата	Краткое содержание документа
Должность	Код исполнителя	Тип документа
Подразделение	Факт исполнения	Организация-отправитель
Дата приема на работу		Код исполнителя

Лабораторная работа 11. Копирование и перенос на другой сервер БД

Для просмотра, запуска, останова служб MS SQL Server необходимо запустить утилиту **SQL Server Configuration Manager** (рис.1).

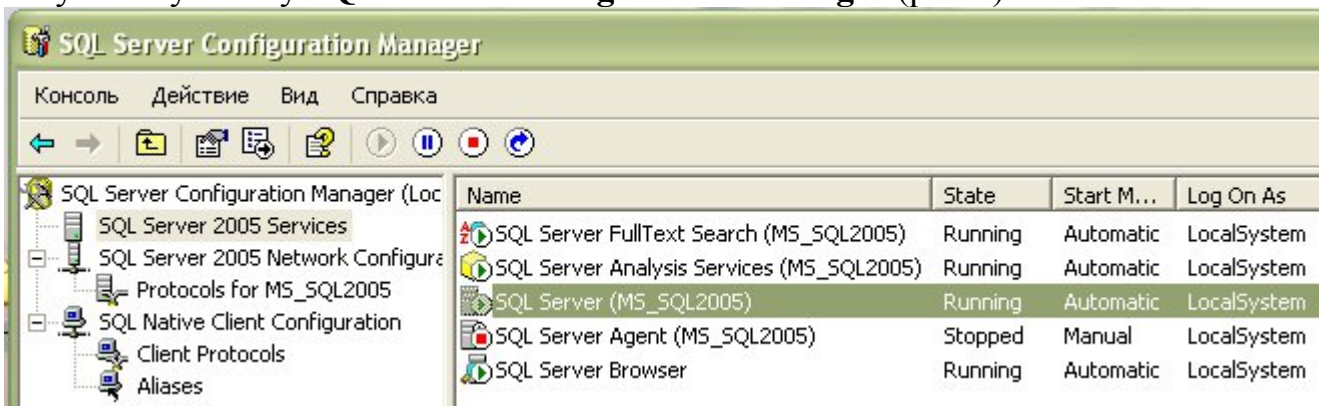

Рис.1 Список служб сервера БД

Для того **чтобы скопировать БД** необходимо остановить службу **SQL Server** (в ее контекстном меню выбрать **Stop**). Далее в подпапке …\MSSQL.1\MSSQL\Data\ скопировать файлы с вашим названием БД (по умолчанию их два). Не забудьте потом снова запустить службу **SQL Server** (в ее контекстном меню выбрать **Start**).

Для того **чтобы подключить** скопированную **БД** на другом сервере, нужно предварительно скопировать ваши файлы в папку …\MSSQL.1\MSSQL\Data\ соответствующего сервера. Далее запустить утилиту **SQL Server Management Studio.** В появившемся окне с названием **Object Explorer** (его можно вызвать по <**F8**>) выбираем **DataBases** (**Базы данных**) и по <правой кнопке мыши> в контекстном меню (рис. 2) выбираем **Attach…** (**Присоединить…**). В

появившемся окне **Attach DataBases** нажать <**Add**> и выбрать ваш файл БД с расширением **.mdf**.

Создание резервной копии БД

1. В контекстном меню вашей БД выбрать Tasks/ Back Up

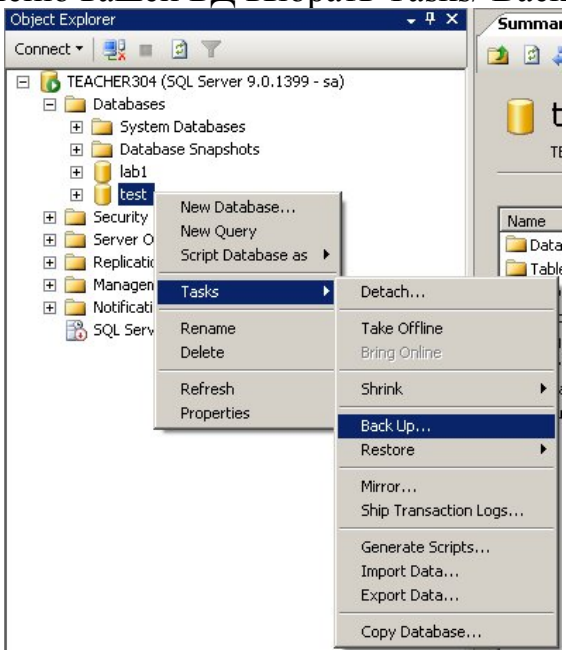

Рис. 2.

2. В появившемся окне **Back Up Database** в разделе **Destination** кнопкой Remove удалить все пути к резервной копии.
3. В окне **Back Up Database** Кнопкой **Add** вызвать проводник, в котором указать путь и название файла, в который будет помещена резервная копия.

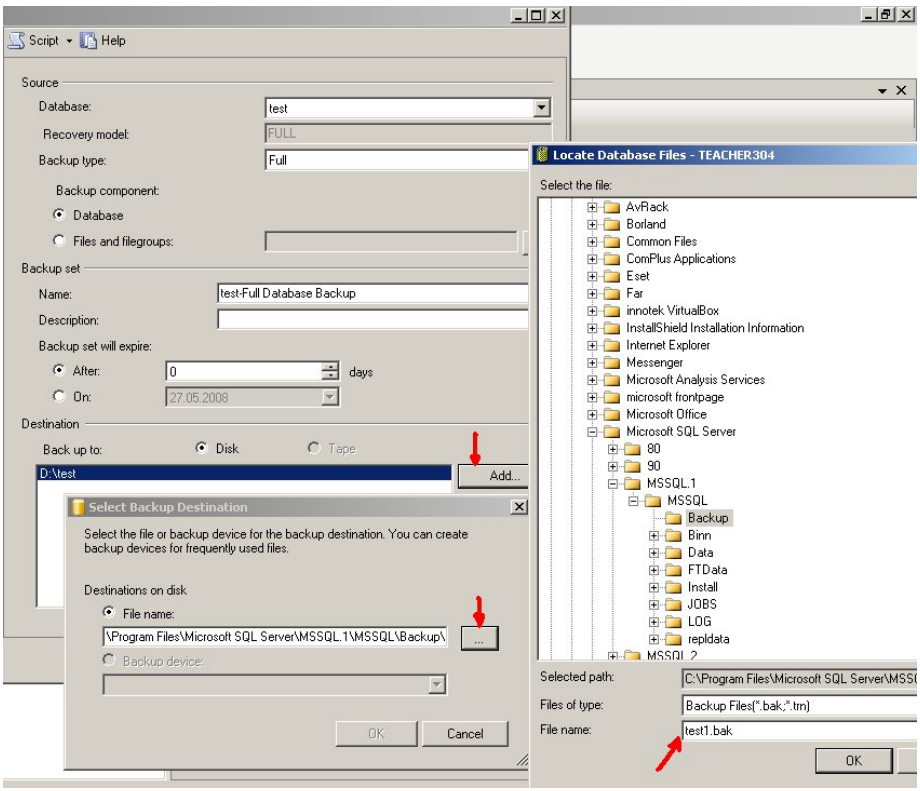

Рис. 3

4. После выбора пути и файла для резервной копии в окне **Back Up Database** нажатием на **OK** запускаем процесс создания резервной копии. В случае успешной работы появится сообщение:

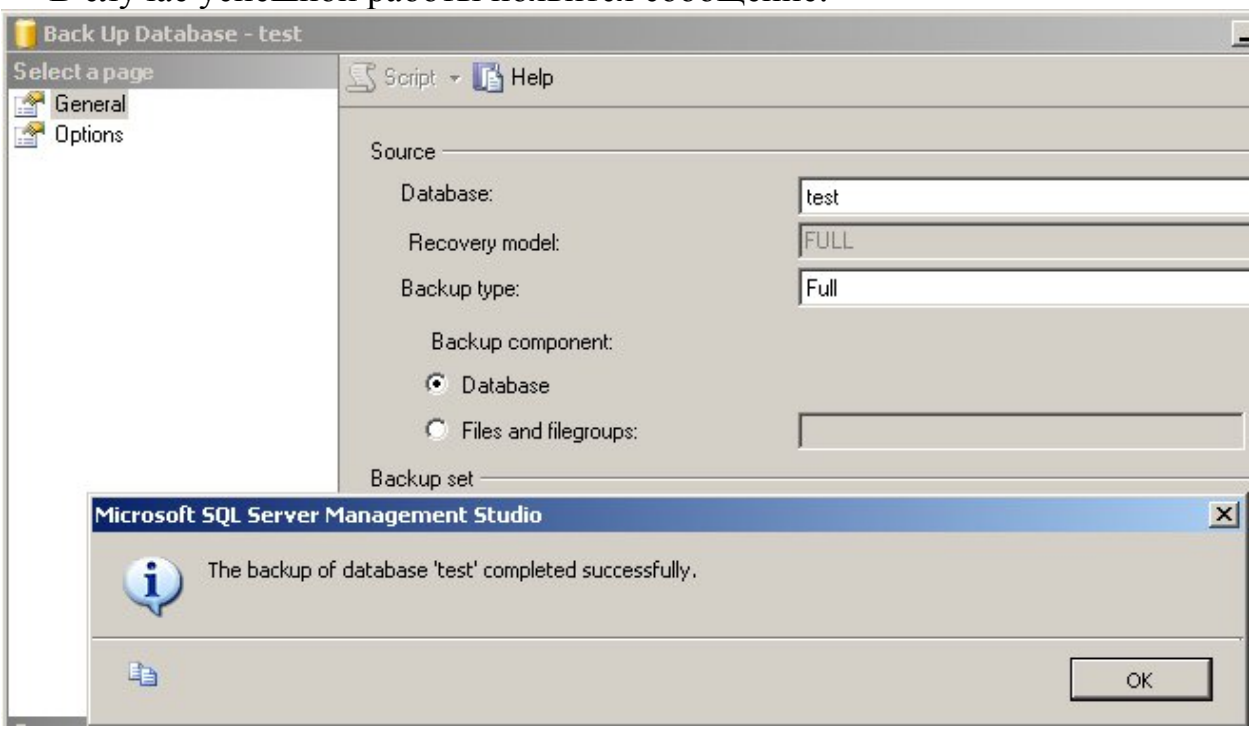

Рис. 4

Восстановление из резервной копии БД

1. В разделе **Databases** в контекстном меню выбираем **Restore Database…**

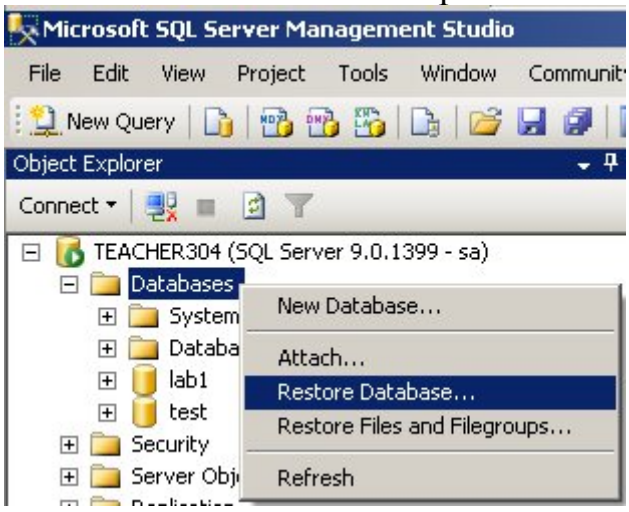

Рис. 5

2. В окне **Restore Database** в разделе **To Database** написать имя новой БД, в которую будет помещен результат, способ восстановления выбирается **From Device**, в следующем окне **Specify Backup** кнопкой **Add** вызываем проводник, в котором указываем путь и имя файла с резервной копией.

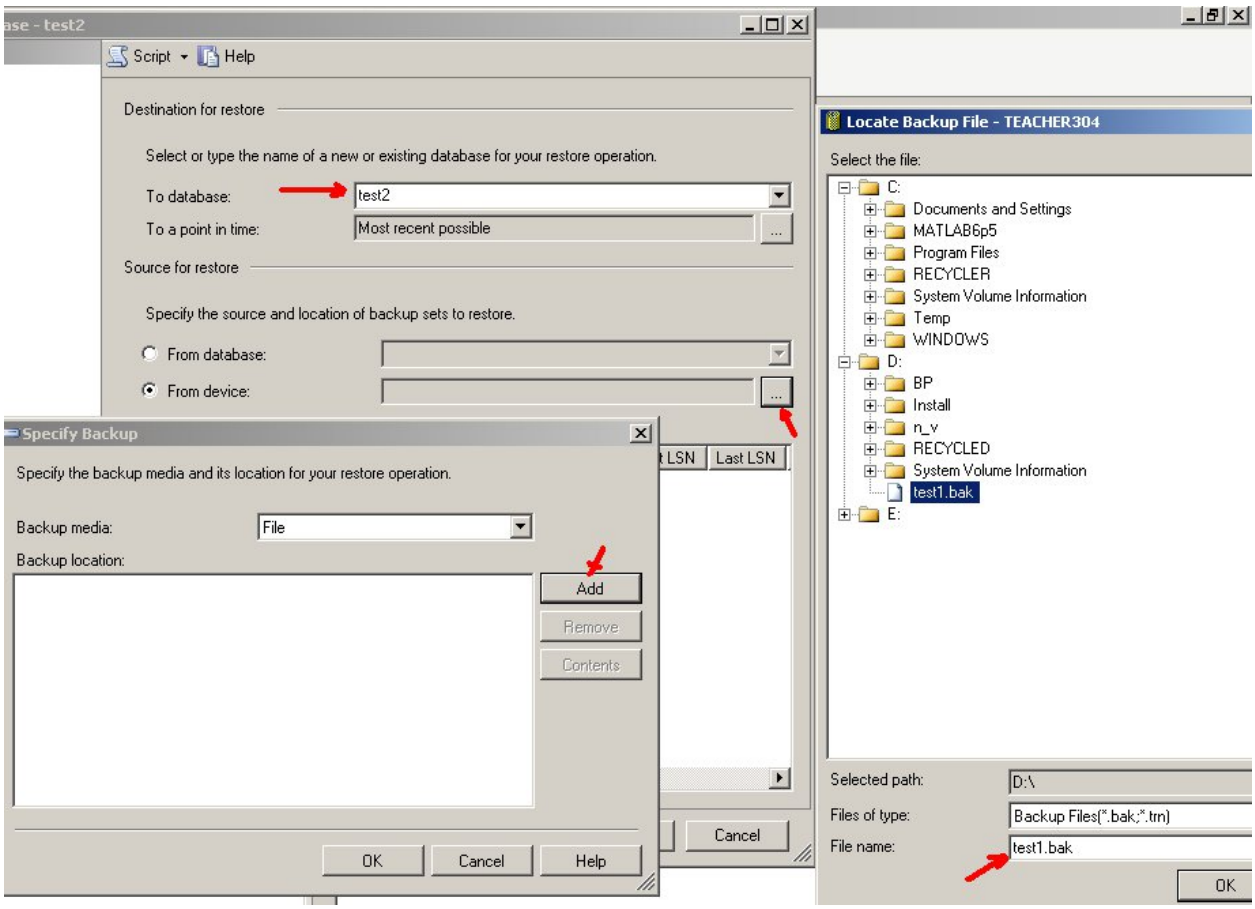

Рис. 6

3. После возврата в окно **Restore Database** в списке **Select the backup sets to restore** отмечаем выбранную резервную копию.

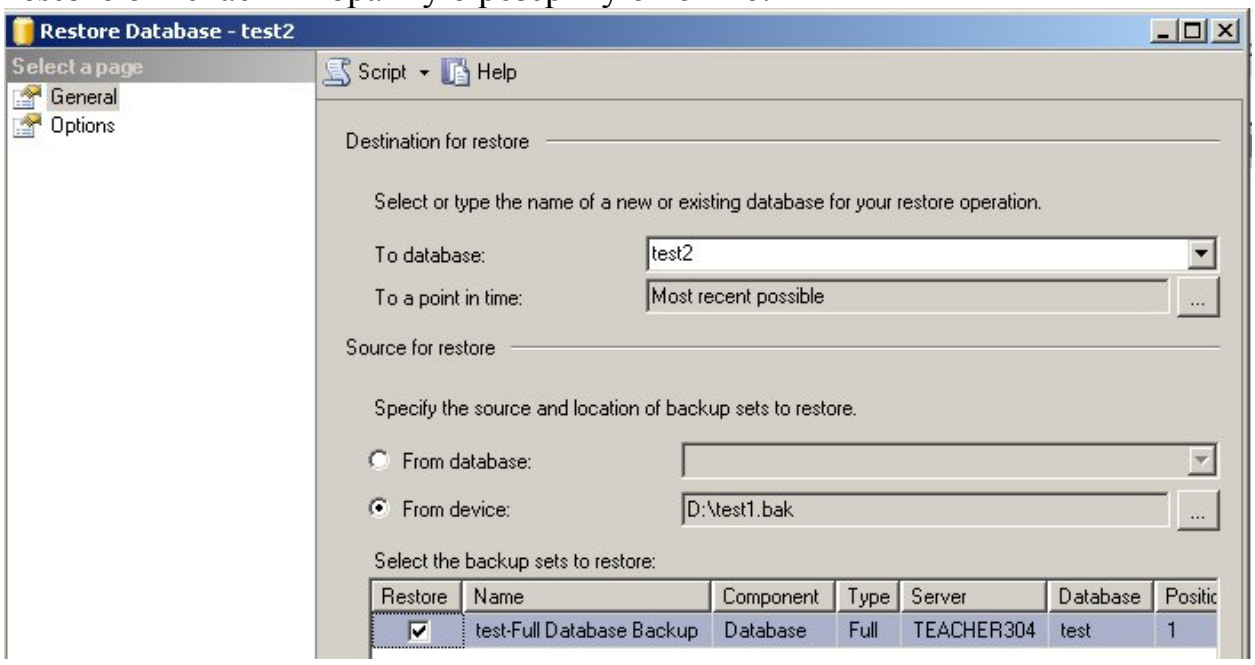

Рис 7.

5. Запускаем процесс восстановления. В случае успешного выполнения получим:

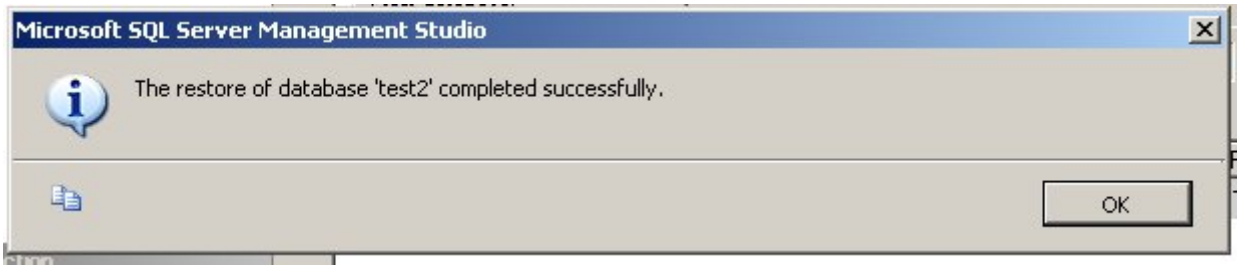

Рис.8

Задания к лабораторной работе

1. Для разработанной базы данных по дисциплине «Информационная безопасность» создать резервную копию
2. Запустить данную копию на другом сервере.
3. Продемонстрировать этапы восстановлению БД из резервной копии.

Лабораторная работа 12. Управление ролями и разрешениями в Microsoft SQL Server

Список системных процедур и команд, которые позволяют реализовать политику разделения прав между пользователя БД.

Название встроенной процедуры	**Описание**
sp_grantlogin	– позволяет использовать пользователей или группы ОС для соединения с Microsoft SQL Server™ , используя Windows Authentication. Этот пример позволяет пользователю Windows NT Corporate\BobJ соединяться с SQL Server. EXEC sp_grantlogin 'Corporate\BobJ'
sp_defaultdb	Изменяет для пользователя БД по умолчанию Этот пример настраит БД по умолчанию pubs для пользователя Victoria. EXEC sp_defaultdb 'Victoria', 'pubs'
sp_grantdbaccess	Добавляет учетную запись из раздела security в текущую БД, для учетных записей Microsoft Windows также дает разрешение на доступ к текущей БД. Синтаксис: EXEC sp_grantdbaccess [@loginame =] 'login' [,[@name_in_db =] 'name_in_db' [OUTPUT]] Этот пример добавляет учетную запись Corporate\GeorgeW в текущую БД и присваивает псевдоним внутри БД Georgie. EXEC sp_grantdbaccess 'Corporate\GeorgeW', 'Georgie'
sp_revokedbaccess	Удаляет информацию об учетной записи из текущей БД. Синтаксис: EXEC sp_revokedbaccess [@name_in_db =] 'name' Этот пример удаляет учетную запись Corporate\GeorgeW из текущей БД. EXEC sp_revokedbaccess 'Corporate\GeorgeW'
sp_addrole	Создает новую роль в текущей БД. Этот пример создает новую роль в текущей БД с названием Managers. EXEC sp_addrole 'Managers'
sp_addrolemember	В текущей БД назначает роль конкретному пользователю. Пример А. Этот пример добавляет учетную запись Corporate\JeffL из Windows NT в БД Sales как пользователя Jeff. Jeff

Название встроенной процедуры	**Описание**
	затем получает роль Sales_Managers в БД Sales. USE Sales --сделать текущей БД Sales GO –выполнить команду, а потом запустить следующую EXEC sp_grantdbaccess 'Corporate\JeffL', 'Jeff' GO EXEC sp_addrolemember 'Sales_Managers', 'Jeff' Пример B. Этот пример добавляет пользователя SQL Server с именем Michael к роли Engineering в текущей БД. EXEC sp_addrolemember 'Engineering', 'Michael'
sp_helprotect	Показывает список привилегий, ассоциированных с ролью.
sp_helprolemember	Показывает список пользователей БД, входящих в указанную роль
sp_addsrvrolemember	Присвоение встроенной серверной роли для существующей учетной записи sp_addsrvrolemember [@loginame =] 'login' , [@rolename =] 'role' Например: sp_addsrvrolemember 'Admin_DB', 'sysadmin'
sp_dropsrvrolemember	Удаление встроенной серверной роли для учетной записи или группы sp_dropsrvrolemember [@loginame =] 'login' , [@rolename =] 'role' Например: sp_dropsrvrolemember 'Admin_DB' , 'sysadmin'
sp_helpsrvrole	Описание только встроенных ролей в SQL Server sp_helpsrvrole [[@srvrolename =] 'role'] Например: sp_helpsrvrole 'sysadmin'
sp_helpsrvrolemember	Возвращает список ролей и учетных записей, которым присвоены эти роли sp_helpsrvrolemember [[@srvrolename =] 'role'] Например: sp_helpsrvrolemember 'sysadmin'
sp_srvrolepermission	Возвращает список ролей и разрешений, которые присвоены этим ролям sp_srvrolepermission [[@srvrolename =] 'role'] Например:

Название встроенной процедуры	Описание
	sp_srvrolepermission 'sysadmin'
sp_addlogin sp_adduser	Создание новой учетной записи в SQL Server в разделе Sequrity: sp_addlogin [@loginame =] 'login' [, [@passwd =] 'password'] [, [@defdb =] 'database'] [, [@deflanguage =] 'language'] [, [@sid =] sid] [, [@encryptopt =] 'encryption_option'] Например: sp_addlogin 'login1',sysname, 'DB_Books' Создает пользователя в SQL Server без PUBLIC в БД ' DB_Books'. Нужно еще использовать sp_adduser [@loginame =] 'login' [, [@name_in_db =] 'user'] [, [@grpname =] 'group'], Пример: Создана база данных DB_Books. В ней создан пользователь Admin_DB с серверной ролью sysadmin, с ролью в БД db_owner. Создать в QueryAnalyzer нового пользователя с именем Public_ и паролем Public_1 (пароль не должен совпадать с именем пользователя) с помощью следующих команд (не забудьте нажать F5 для запуска команд на выполнение): EXEC sp_addlogin 'Public_','Public_1', 'DB_Books' use DB_Books EXEC sp_adduser 'Public_','Public_' В БД DB_Books создан пользователь Public_ с ролью в БД DB_Books public.
Deny (отрицание)	Этот пример запрещает несколько системных привилегий для нескольких пользователей. Пользователи не могут использовать системные привилегии CREATE DATABASE or CREATE TABLE, если они не наделены имим через команду GRANT. Пример:

Название встроенной процедуры	Описание
	DENY CREATE DATABASE, CREATE TABLE TO Mary, John, [Corporate\BobJ] DENY SELECT, INSERT, UPDATE, DELETE ON authors TO Mary, John, Tom

Создание пользователей на доступ к серверу через утилиту **Microsoft SQL Server Management Studio**

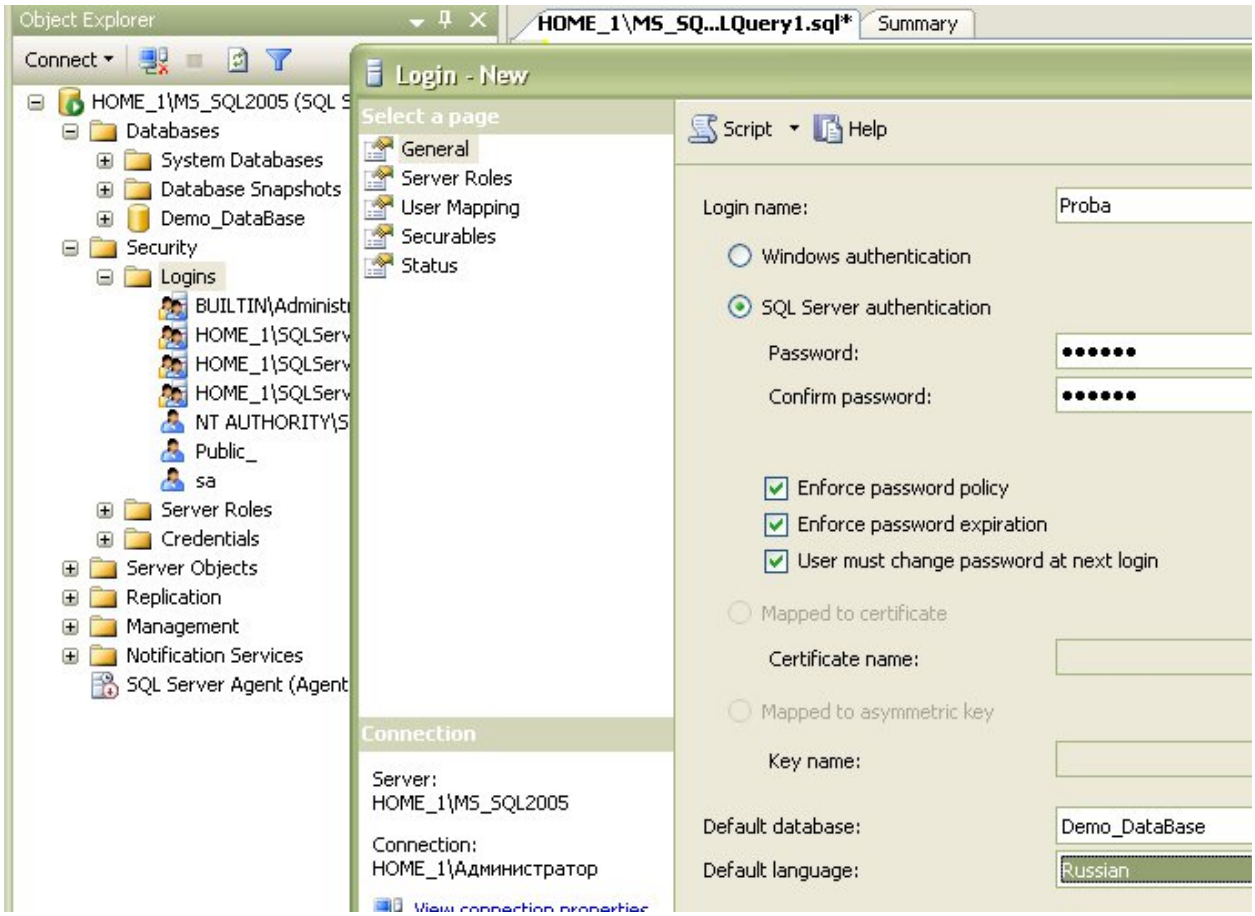

Рис. 9. Раздел Security для работы с пользователями и создание нового пользователя (при SQL Server аутентификации нужно снять галочки с **Enforce password policy**)

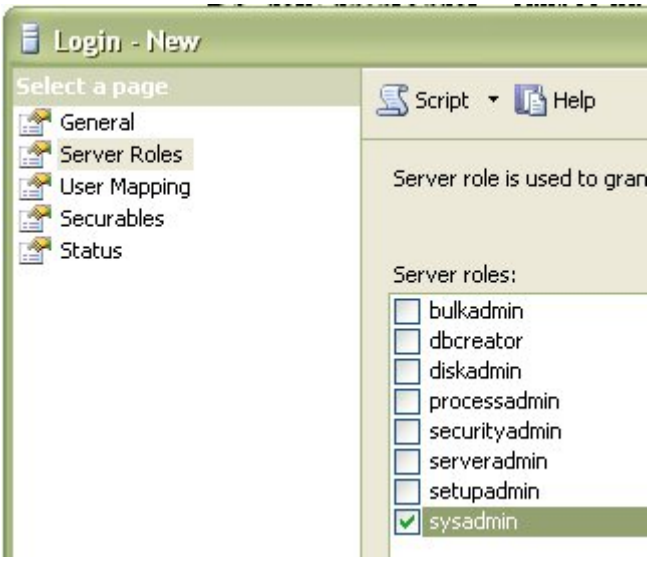

Рис. 10 Настройка серверной роли для нового пользователя (весь список серверных ролей с их привилегиями в конце работы)

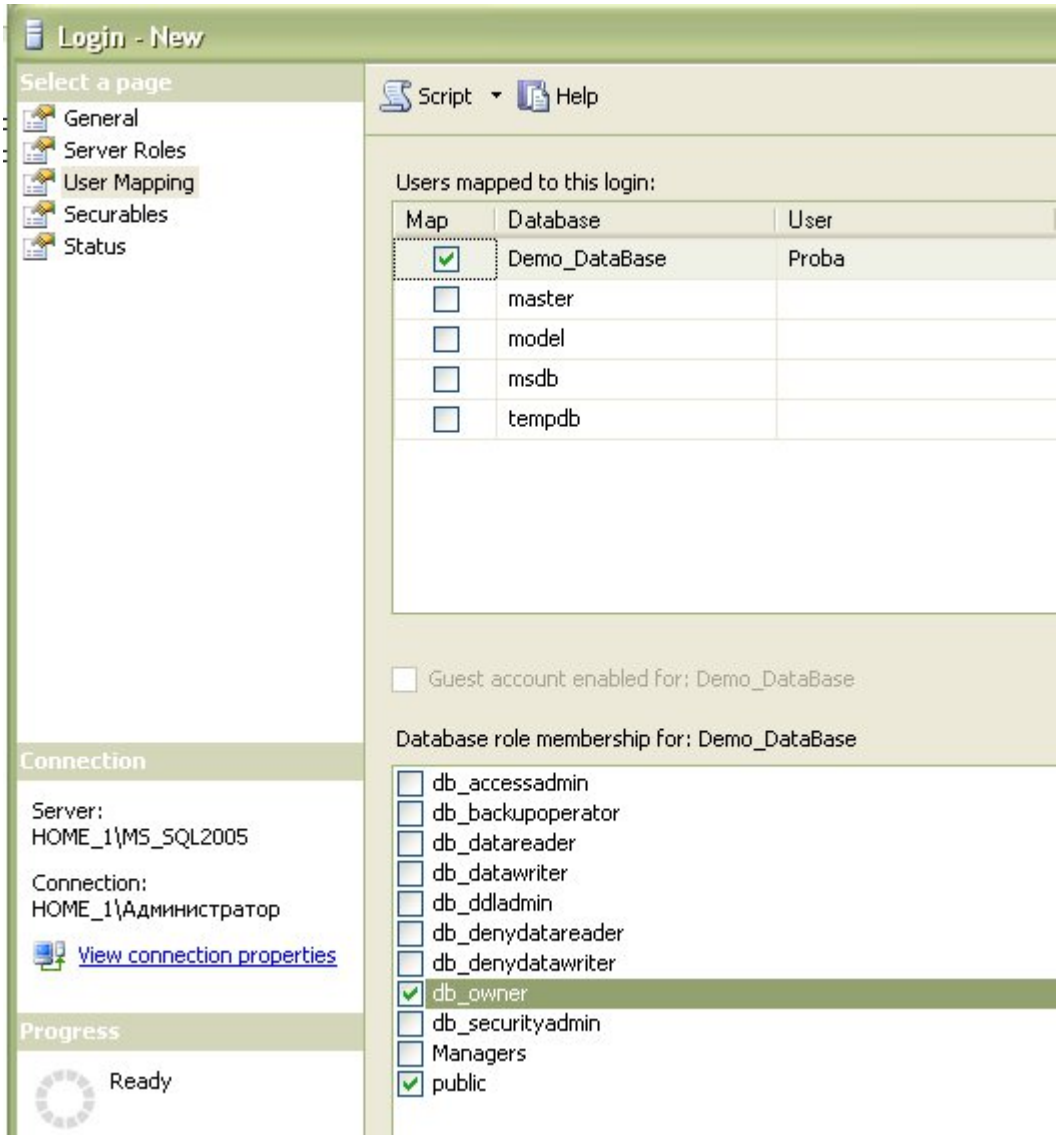

Рис. 11 Настройка роли базы данных для нового пользователя (весь список ролей баз данных с их привилегиями ниже)

Перечень ролей БД:
Public – минимальные права доступа к БД (на просмотр)
Db_owner – может выполнять любые действия с БД
Db_accessadmin – добавляет и удаляет пользователей БД
Db_sequrityadmin – управляет ролями в Бди разрешениями на запуск команд и работу с объектами БД
Db_ddladmin – добавляет, изменяет и удаляет объекты БД
Db_backupoperator – осуществляет резервное копирования БД
Db_datareader – может просматривать все данные в каждой таблице в БД
Db_datawriter - может добавлять, удалять и изменять данные в каждой таблице в БД
Db_denydatareader – запрет на просмотр всех данных в каждой таблице в БД
Db_denydatawriter - запрет на добавление, удаление и изменение всех данных в каждой таблице в БД

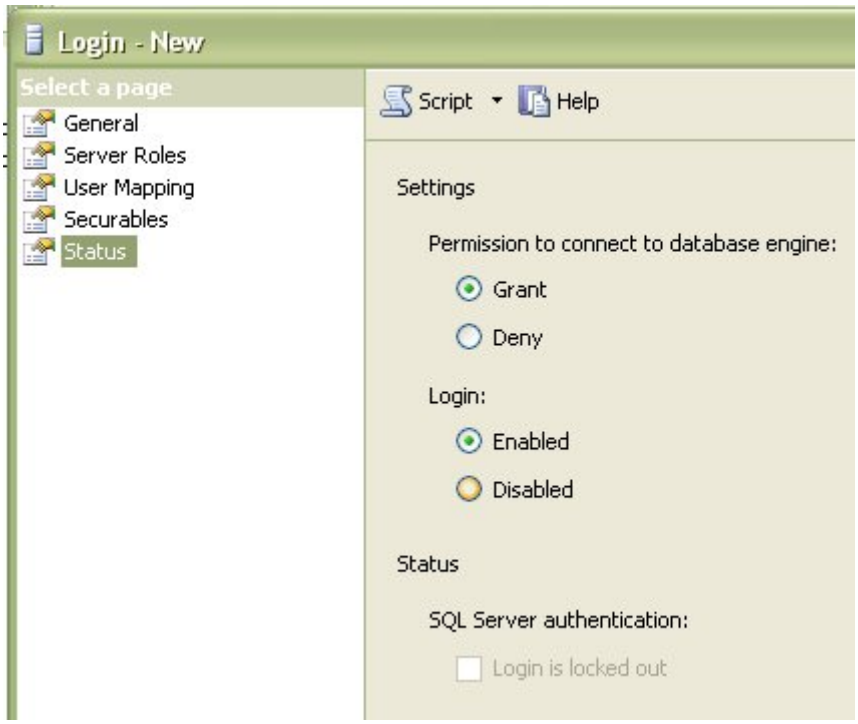

Рис. 12. Разблокирование создаваемой учетной записи

После нажатия на <OK> в БД появится пользователь **Proba** с правами собственника БД, который может выполнять все манипуляции с БД **Demo_DataBase**.

Создание ролей программно

Для упрощения управления правами доступа в системе создаются роли, которые затем можно назначать группе пользователей.
Создадим для нашего примера роли библиотекаря (LIBRAR) и читателя (READER).
Пример создания роли библиотекаря:

USE Demo_DataBase --сделать текущей БД Demo_DataBase
EXEC sp_addrole 'LIBRAR'

Эти операторы набрать на странице, вызванной нажатием кнопки <**New Query**> (<**Новый запрос**>) или через пункт меню **File**/ **New**/ **Query in current connection** или нажатием комбинации клавиш **<CTRL>+ <N>**.

Для запуска команд на выполнение нажать <**F5>**.

Повторный запуск тех же команд сгенерирует ошибки типа «В БД уже существует роль LIBRAR».

Пример создания роли читателя:
USE Demo_DataBase --сделать текущей БД Demo_DataBase
EXEC sp_addrole 'READER'

Библиотекарь должен обладать правами на чтение, удаление, изменение, добавление во все таблицы БД Demo_DataBase, а также должен иметь возможность запускать на исполнение процедуры и функции БД Demo_DataBase. Поэтому роли библиотекаря из системных привилегий назначаем EXECUTE, а из привилегий доступа к объектам назначаем DELETE, INSERT, UPDATE, SELECT.
Читатель должен обладать правами на чтение из таблиц ADMIN_BOOKS.AUTHORS, ADMIN_BOOKS.BOOKS, ADMIN_BOOKS.PUBLISHING_HOUSE. Поэтому роли читателя из привилегий доступа к объектам назначаем SELECT.

Оператор представления привилегий

Синтаксис:
GRANT <привилегия>, ...
ON < объект >, …
TO <имя>
[WITH grant option];

Атрибут **WITH GRANT OPTION** дает право пользователю самому раздавать права, которые он получил.
С помощью оператора **GRANT** для каждого пользователя формируется список привилегий, привилегии управляют работой сервера данных с точки зрения защиты данных. Выполнению каждой транзакции предшествует проверка привилегий пользователя, сеанс которого породил транзакцию.

Пример: GRANT select, update (Sales, num) ON Sales_data TO user1
WITH GRANT OPTION
Пользователь, предоставивший привилегию другому называется грантор (grantor — предоставитель). Привилегия является предоставляемой, если право на нее можно предоставить другим пользователям.

PUBLIC — имя роли, которую получает пользователь при добавлении в список пользователей конкретной БД, включает в себя минимальный набор прав на чтение данных из таблиц и представлений в БД.
Роль библиотекаря названа LIBRAR. Операторы назначения прав доступа для этой роли представлены ниже:
GRANT DELETE, INSERT, UPDATE, SELECT ON BOOKS TO LIBRAR
GRANT DELETE, INSERT, UPDATE, SELECT ON AUTHORS TO LIBRAR
GRANT DELETE, INSERT, UPDATE, SELECT ON DELIVERIES TO LIBRAR
GRANT EXECUTE TO LIBRAR

Роль читателя названа READER. Операторы назначения прав доступа для этой роли представлены ниже:
GRANT SELECT ON BOOKS TO READER
GRANT SELECT ON AUTHORS TO READER
GRANT SELECT ON PUBLISHING_HOUSE TO READER

Создание пользователей с определенной ролью

Пример создания библиотекаря Ivanov_Lib и присвоения ему роли:
EXEC sp_addlogin '**Ivanov_Lib**','**Ivanov**', 'Demo_DataBase'
use Demo_DataBase
EXEC sp_adduser '**Ivanov_Lib**','**Ivanov_Lib**'
EXEC sp_addrolemember 'LIBRAR', '**Ivanov_Lib**'

Пример создания читателя Petrov_Read и присвоения роли:
EXEC sp_addlogin '**Petrov_Read**','**Petrov**', 'Demo_DataBase'
use Demo_DataBase
EXEC sp_adduser '**Petrov_Read**','**Petrov_Read**'
EXEC sp_addrolemember 'READER', '**Petrov_Read**'

Оператор отмены привилегий

Синтаксис отмены привилегий:
REVOKE [with grant option]
< привилегии >,…
ON < объект >,…
FROM <имя_пользователя>;
Предложение **with grant option** сохраняет за пользователем перечисленные привилегии, но отменяет его право передавать их кому-либо другому.
Пример:
REVOKE SELECT ON AUTHORS FROM READER

Оператор изымания роли у пользователя:
Revoke <список ролей> from <список пользователей>.
Пример:
use Demo_DataBase
EXEC sp_droprolemember 'READER', 'Petrov_Read'

Варианты заданий к лабораторной работе №2

Общие положения

В утилите **SQL Server Management Studio** выполнить примеры, которые даны по ходу работы.

По индивидуальному варианту базы данных, которая выполнена в 1 лабораторной работе, *определить 2-3 должностных лица*, которые могут работать с таблицами БД. Для каждого должностного лица определить набор привилегий, которыми он может пользоваться.

В утилите **SQL Server Management Studio** создать под каждое должностное лицо соответствующую роль, наделить эту роль определенными привилегиями. Далее создать по одному пользователю на каждую должность и присвоить им соответствующие роли.

Сохранить последовательно операторы с указанием заданий в файле с названием **ФамилияСтудента_Лаб_2_№варианта_общее.** Операторы создания ролей, привилегий и пользователей сохранить в файле с названием **ФамилияСтудента_Лаб_2_№варианта.**

Справочная информация

Для просмотра служебной информации можно обратиться к системным представлениям, как показано на рис. 4.5. в разделе **Object Explorer**. Также на рис. 13. показаны три команды и результат их выполнения, которые позволяют увидеть списки созданных пользователей и ролей всех БД; объектов, созданных на сервере; учетных записей с SQL Server аутентификацией.

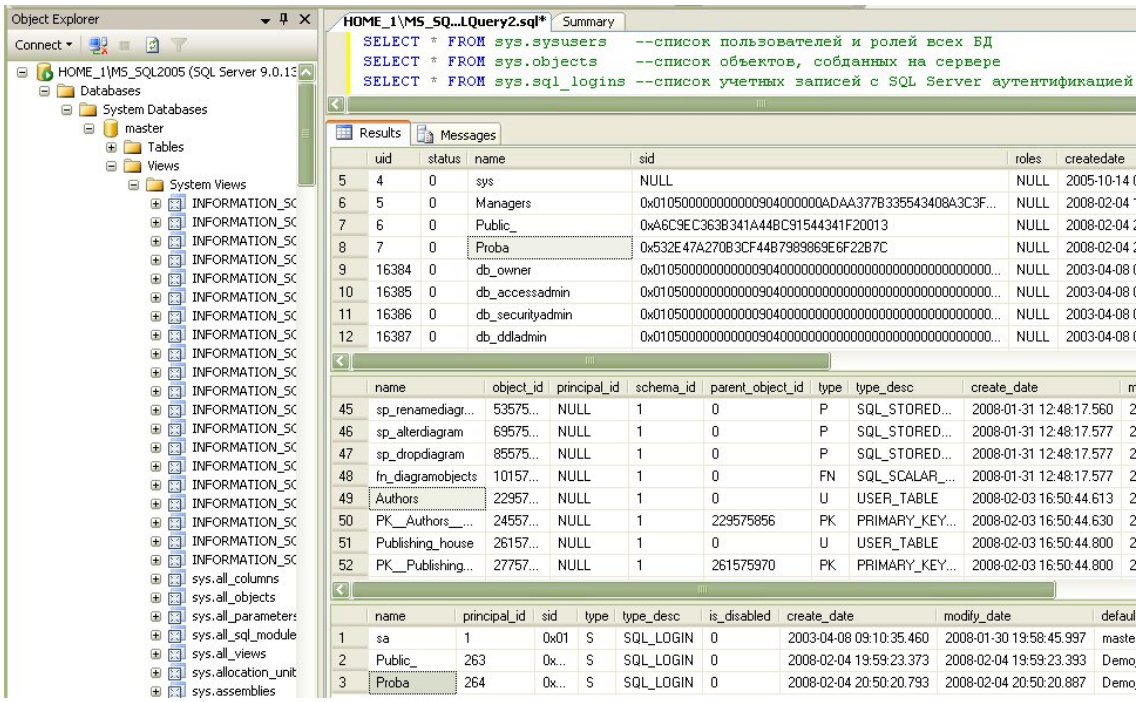

Рис. 13.

Список разрешений для роли sysadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'sysadmin'**

sysadmin Add extended procedures
sysadmin Add member to bulkadmin
sysadmin Add member to dbcreator
sysadmin Add member to diskadmin
sysadmin Add member to processadmin
sysadmin Add member to securityadmin
sysadmin Add member to serveradmin
sysadmin Add member to setupadmin
sysadmin Add member to sysadmin
sysadmin Add/drop to/from db_accessadmin
sysadmin Add/drop to/from db_backupoperator
sysadmin Add/drop to/from db_datareader
sysadmin Add/drop to/from db_datawriter
sysadmin Add/drop to/from db_ddladmin
sysadmin Add/drop to/from db_denydatareader

sysadmin Add/drop to/from db_denydatawriter
sysadmin Add/drop to/from db_owner
sysadmin Add/drop to/from db_securityadmin
sysadmin Add/drop/configure linked servers
sysadmin All DDL but GRANT, REVOKE, DENY
sysadmin ALTER DATABASE
sysadmin BACKUP DATABASE
sysadmin BACKUP LOG
sysadmin BULK INSERT
sysadmin CHECKPOINT
sysadmin Complete SETUSER SQL user
sysadmin Constraints on System tables
sysadmin CREATE DATABASE
sysadmin Create indices on system tables
sysadmin Create/delete/modify system tables
sysadmin dbcc change 'on' rules
sysadmin dbcc checkalloc
sysadmin dbcc checkdb
sysadmin dbcc checkfilegroup
sysadmin dbcc checkident
sysadmin dbcc checktable
sysadmin dbcc cleantable
sysadmin dbcc dbreindex
sysadmin dbcc dropcleanbuffers
sysadmin dbcc freeproccache
sysadmin dbcc inputbuffer
sysadmin dbcc outputbuffer
sysadmin dbcc pintable
sysadmin dbcc proccache
sysadmin dbcc setcpuweight
sysadmin dbcc setioweight
sysadmin dbcc show_statistics
sysadmin dbcc showcontig
sysadmin dbcc showoptweights
sysadmin DBCC ShrinkDatabase
sysadmin dbcc shrinkfile
sysadmin dbcc traceon/off
sysadmin dbcc updateusage
sysadmin DELETE permission on any object
sysadmin DENY
sysadmin DISK INIT
sysadmin DROP DATABASE
sysadmin EXECUTE any procedure
sysadmin Extend database
sysadmin GRANT

sysadmin Grant/deny/revoke CREATE DATABASE
sysadmin INSERT permission on any object
sysadmin KILL
sysadmin Mark a stored procedure as startup
sysadmin Raiserror With Log
sysadmin Read the error log
sysadmin RECONFIGURE
sysadmin REFERENCES permission on any table
sysadmin RESTORE DATABASE
sysadmin RESTORE LOG
sysadmin REVOKE
sysadmin SELECT permission on any object
sysadmin SHUTDOWN
sysadmin sp_addalias
sysadmin sp_addapprole
sysadmin sp_addgroup
sysadmin sp_addlinkedsrvlogin
sysadmin sp_addlogin
sysadmin sp_addrole
sysadmin sp_addrolemember
sysadmin sp_addumpdevice
sysadmin sp_adduser
sysadmin sp_altermessage
sysadmin sp_approlepassword
sysadmin sp_change_users_login
sysadmin sp_changedbowner
sysadmin sp_changegroup
sysadmin sp_changeobjectowner
sysadmin sp_configure
sysadmin sp_dbcmptlevel
sysadmin sp_dboption (update)
sysadmin sp_dboption update part
sysadmin sp_defaultdb
sysadmin sp_defaultlanguage
sysadmin sp_denylogin
sysadmin sp_diskdefault
sysadmin sp_dropalias
sysadmin sp_dropapprole
sysadmin sp_dropdevice
sysadmin sp_dropgroup
sysadmin sp_droplinkedsrvlogin
sysadmin sp_droplogin
sysadmin sp_dropremotelogin
sysadmin sp_droprole
sysadmin sp_droprolemember

sysadmin	sp_dropuser
sysadmin	sp_fulltext_catalog
sysadmin	sp_fulltext_column
sysadmin	sp_fulltext_database
sysadmin	sp_fulltext_service
sysadmin	sp_fulltext_table
sysadmin	sp_grantdbaccess
sysadmin	sp_grantlogin
sysadmin	sp_helplogins
sysadmin	sp_password
sysadmin	sp_recompile
sysadmin	sp_refreshview
sysadmin	sp_remoteoption
sysadmin	sp_remoteoption (update)
sysadmin	sp_rename
sysadmin	sp_renamedb
sysadmin	sp_revokedbaccess
sysadmin	sp_revokelogin
sysadmin	sp_tableoption
sysadmin	sp_updatestats
sysadmin	TRUNCATE TABLE
sysadmin	UPDATE permission on any object
sysadmin	USE to a suspect database

Список разрешений для роли securityadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'securityadmin'**

Securityadmin	Add member to securityadmin
securityadmin	Grant/deny/revoke CREATE DATABASE
securityadmin	Read the error log
securityadmin	sp_addlinkedsrvlogin
securityadmin	sp_addlogin
securityadmin	sp_defaultdb
securityadmin	sp_defaultlanguage
securityadmin	sp_denylogin
securityadmin	sp_droplinkedsrvlogin
securityadmin	sp_droplogin
securityadmin	sp_dropremotelogin
securityadmin	sp_grantlogin
securityadmin	sp_helplogins
securityadmin	sp_password
securityadmin	sp_remoteoption (update)
securityadmin	sp_revokelogin

Список разрешений для роли serveradmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'serveradmin'**

serveradmin Add member to serveradmin
serveradmin dbcc freeproccache
serveradmin RECONFIGURE
serveradmin SHUTDOWN
serveradmin sp_configure
serveradmin sp_fulltext_service
serveradmin sp_tableoption

Список разрешений для роли setupadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'setupadmin'**

setupadmin Add member to setupadmin
setupadmin Add/drop/configure linked servers
setupadmin Mark a stored procedure as startup

Список разрешений для роли processadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'processadmin'**

processadmin Add member to processadmin
processadmin KILL

Список разрешений для роли diskadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'diskadmin'**
diskadmin Add member to diskadmin
diskadmin DISK INIT
diskadmin sp_addumpdevice
diskadmin sp_diskdefault
diskadmin sp_dropdevice

Список разрешений для роли dbcreator

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'dbcreator'**

dbcreator Add member to dbcreator
dbcreator ALTER DATABASE
dbcreator CREATE DATABASE
dbcreator DROP DATABASE
dbcreator Extend database

dbcreator RESTORE DATABASE
dbcreator RESTORE LOG
dbcreator sp_renamedb

Список разрешений для роли bulkadmin

Можно посмотреть с помощью: **EXEC sp_srvrolepermission 'bulkadmin'**

bulkadmin Add member to bulkadmin
bulkadmin BULK INSERT

Лабораторная работа 13. Администрирование SQL сервера

Цель работы: изучить основные функции и механизмы, заложенные в СУБД на примере MS SQL Server, позволяющие поддерживать БД в работоспособном состоянии.

Контрольные точки и их создание

Возможность создания *контрольных точек* была включена в SQL Server с целью фиксации изменений в базе данных или параметрах настройки в заранее заданный удобный момент времени. Если производилась настройка сервера или в его функционирование вносились изменения, потребовавшие перезагрузки управляющей программы, это значит, наступил момент для ручного запуска процедуры создания контрольной точки.

После запуска процедуры создания контрольной точки (независимо от способа ее вызова – вручную или посредством автоматического процесса) все модифицированные страницы памяти сбрасываются на диск. *Модифицированная страница* – это такая страница памяти, которая содержит изменения в данных, еще не зафиксированные в образе базы данных на жестком диске. По умолчанию процедура создания контрольной точки автоматически запускается приблизительно каждые 60 секунд. Реальный промежуток времени между двумя контрольными точками определяется текущей загрузкой сервера, заданными параметрами защиты от сбоев и текущими установками общей настройки производительности SQL Server. Однако этот реальный промежуток времени будет достаточно близок к 60 секундам.

Вероятно, вы уже заметили, что если SQL Server неожиданно прекратил работу в результате случайного сбоя, то на его повторный запуск может потребоваться достаточно много времени. Это происходит по той причине, что SQL Server осуществляет откат и повторное выполнение всех транзакций, которые происходили после создания последней контрольной точки. При этом база данных предварительно приводится в последнее, известное системе, корректное состояние. Оно соответствует именно тому моменту, когда был запущен и успешно завершен процесс создания последней контрольной точки.

Работа SQL Server может быть в любой момент остановлена с помощью выдачи команды shutdown. Если перед выдачей этой команды ввести команду checkpoint, то все внесенные в результате последних транзакций изменения будут корректно зафиксированы в базе данных до остановки ее работы.

Если по какой-либо причине предстоит остановить работу SQL Server (особенно если требуется указать параметр WITH NOWAIT), то можно избежать продолжительной процедуры последующего запуска системы, предварительно вручную выдав команду CHECKPOINT. Выполнение этой команды ни чем не отличается от процедуры создания контрольной точки, вызванной автоматически. Вся информация будет сохранена на диске и запуск системы будет сведен к простой загрузке программ ядра базы данных и предоставления доступа к данным всем клиентским приложениям. Это

замечание особенно полезно в тех случаях, когда необходима экстренная остановка сервера – например, при отказе системы электропитания и наличии источника бесперебойного питания, способного обеспечить функционирование сервера на время, достаточное для выполнения цикла создания контрольной точки.

Команда checkpoint выполняется на уровне базы данных и всегда применяется по отношению к текущей базе данных. Если в системе имеется несколько баз данных, эту команду следует выдать для каждой из баз данных в отдельности. Чтобы иметь право выдать команду checkpoint для некоторой базы данных, необходимо иметь статус ее владельца.

Кроме этого, следует упомянуть параметр TRUNCATE LOG ON CHECKPOINT, который также может оказаться довольно полезным. Установка этого параметра вызывает автоматическую очистку журнала транзакций после завершения создания очередной контрольной точки. Таким образом, журнал транзакций будет вестись только в промежутках между созданием контрольных точек. Для установки этого параметра в окне SQL Server Enterprise Manager щелкните правой кнопкой мыши на пиктограмме базы данных и выберите в контекстном меню команду Properties. В раскрывшемся диалоговом окне свойств базы данных перейдите во вкладку Options.

При установленном параметре Truncate log on checkpoint невозможно сделать резервную копию журнала транзакций в процессе выполнения стандартной процедуры резервного копирования базы данных. Обычно это не является проблемой, поскольку стандартное копирование базы данных по-прежнему будет выполняться. Однако данное замечание следует учитывать при планировании процедур копирования. Процесс резервного копирования и восстановления системы подробно обсуждается в последующих разделах этой главы.

Если для некоторой базы данных установлен параметр Truncate log on checkpoint, то ее журнал транзакций будет каждый раз очищаться в момент успешной фиксации последней транзакции (при отсутствии в системе репликации данных). Если в системе используется репликация данных, информация в журнале очищается в момент успешного завершения репликации и фиксации в базе данных последней транзакции. Поскольку процедуры репликации данных используют данные журнала транзакций, информация о проведенной транзакции не удаляется из журнала до тех пор, пока сведения о ней не будут доставлены всем подписчикам данного источника.

Проверка целостности базы данных

```
USE master;
GO
EXEC sp_dboption 'Demo_DataBase', 'read only', 'TRUE';
```

Режимы выполнения команды DBCC

Команда DBCC поддерживает несколько режимов выполнения. В последующих разделах будут рассмотрены те из них, которые используются чаще всего. Кроме того, мы проанализируем, чем они могут помочь в управлении системой SQL Server.

DBCC CHECKALLOC

DBCC CHECKALLOC [('*имя_базы_данных'*[, NOINDEX])] [WITH NO_INFOMSGS]

Если при вызове команды опустить имя базы данных, SQL Server осуществит проверку текущей базы данных. При выполнении команды с указанием режима CHECKALLOC в отчет помещается детальная информация о системе и существующих в ней объектах базы данных. Эту информацию можно использовать для поиска возможных проблем в системе. Обнаруженные проблемы следует изучать и устранять по отдельности. Помещаемая в отчет информация – это сведения о существующей структуре таблиц, распределении страниц памяти и т.п. Каждое сообщение об обнаруженной ошибке обязательно сопровождается конкретными инструкциями по ее устранению.

Пример:

```
USE Demo_DataBase
GO
DBCC CHECKALLOC
```

Результат (фрагмент):

```
DBCC results for 'Demo_DataBase'.
*****************************************************
******
Table sys.sysrowsetcolumns                Object ID 4.
Index ID 1, partition ID 262144, alloc unit ID 262144
(type In-row data). FirstIAM (1:139). Root (1:66). Dpages
5.
Index ID 1, partition ID 262144, alloc unit ID 262144
(type In-row data). 7 pages used in 0 dedicated extents.
Total number of extents is 0.
*****************************************************
******
...

CHECKALLOC found 0 allocation errors and 0 consistency
errors in database 'Demo_DataBase'.
DBCC execution completed. If DBCC printed error messages,
contact your system administrator.
```

DBCC CHECKDB

При вызове команды DBCC в режиме CHECKDB, на наличие ошибок проверяется каждая таблица и связанные с ней страницы данных, индексы и указатели. Индексы и страницы данных контролируются на предмет корректности установленных связей. Кроме того, индексы дополнительно анализируются на соответствие заданному порядку сортировки. Для каждой страницы проверяется обоснованность данных, целостность указателей и корректность ее формата. Дополнительно в режиме CHECKDB контролируется правильность связей между текстом, графикой и страницами типа NTEXT, а также корректность их размера. Если выполняется вызов команды DBCC в режиме CHECKDB, то повторно запускать ее в режимах CHECKALLOC или CHECKTABLE не потребуется. Команда DBCC в режиме CHECKDB имеет следующий синтаксис:

DBCC CHECKDB [('*имя_базы_данных'*[, NOINDEX])] [WITH NO_INFOMSGS]

Если опустить параметр имени базы данных, будет выполнена проверка текущей базы данных.

Результат (фрагмент) выполнения команды DBCC CHECKDB без параметров для текущей БД Demo_DataBase:

```
DBCC results for 'Demo_DataBase'.
Service Broker Msg 9675, State 1: Message Types analyzed:
14.
Service Broker Msg 9676, State 1: Service Contracts
analyzed: 6.
Service Broker Msg 9667, State 1: Services analyzed: 3.
Service Broker Msg 9668, State 1: Service Queues
analyzed: 3.
Service Broker Msg 9669, State 1: Conversation Endpoints
analyzed: 0.
Service Broker Msg 9674, State 1: Conversation Groups
analyzed: 0.
Service Broker Msg 9670, State 1: Remote Service Bindings
analyzed: 0.
DBCC results for 'sys.sysrowsetcolumns'.
There are 557 rows in 5 pages for object
"sys.sysrowsetcolumns".
DBCC results for 'sys.sysrowsets'.
There are 83 rows in 1 pages for object "sys.sysrowsets".
DBCC results for 'sysallocunits'.
There are 96 rows in 1 pages for object "sysallocunits".
DBCC results for 'sys.sysfiles1'.
There are 2 rows in 1 pages for object "sys.sysfiles1".
DBCC results for 'sys.syshobtcolumns'.
```

```
There are 557 rows in 5 pages for object
"sys.syshobtcolumns".
DBCC results for 'sys.syshobts'.
There are 83 rows in 1 pages for object "sys.syshobts".
...

CHECKDB found 0 allocation errors and 0 consistency
errors in database 'Demo_DataBase'.
DBCC execution completed. If DBCC printed error messages,
contact your system administrator.
```

DBCC CHECKTABLE

Если проверка всей базы данных в целом занимает слишком много времени, можно воспользоваться режимом CHECKTABLE. В этом случае в команде DBCC задается режим CHECKTABLE и указывается перечень имен таблиц базы данных, которые следует проверить. Будет выполнен анализ состояния только указанных таблиц, что позволит сократить общее время проверки.

DBCC CHECKFILEGROUP

При выполнении команды DBCC в режиме CHECKFILEGROUP, проверяется каждая таблица и связанные с ней страницы данных, индексы и указатели. Индексы и страницы данных контролируются на корректность установленных связей. Кроме того, индексы дополнительно анализируются на соответствие заданному порядку сортировки. Для каждой страницы проверяется обоснованность данных, целостность указателей и корректность ее формата. Дополнительно в режиме CHECKFILEGROUP контролируется правильность связей между текстом, графикой и страницами типа NTEXT, а также корректность их размера.

Команда DBCC в режиме CHECKFILEGROUP имеет следующий синтаксис:

```
DBCC CHECKFILEGROUP [(([{'filegroup_name' | filegroup_id |
0 } ] [ , NOINDEX ])]
    [ WITH {[ ALL_ERRORMSGS ][ NO_INFOMSGS ] ] [ ,
[ TABLOCK ] ]
    [ , [ ESTIMATEONLY ] ] }]
```

Операторы, выводящие информацию о БД

DBCC CONCURRENCYVIOLATION	DBCC SHOW_STATISTICS
DBCC INPUTBUFFER	DBCC SHOWCONTIG
DBCC OPENTDBCC INPUTBUFFERRAN	DBCC SQLPERF
DBCC OUTPUTBUFFER	DBCC TRACESTATUS
DBCC PROCCACHE	DBCC USEROPTIONS

Операторы проверки целостности и корректности данных объектов БД

DBCC CHECKALLOC	DBCC CHECKFILEGROUP
DBCC CHECKCATALOG	DBCC CHECKIDENT
DBCC CHECKCONSTRAINTS	DBCC CHECKTABLE
DBCC CHECKDB	

Операторы очистки и восстановления объектов БД

DBCC CLEANTABLE	DBCC INDEXDEFRAG
DBCC DBREINDEX	DBCC SHRINKDATABASE
DBCC DROPCLEANBUFFERS	DBCC SHRINKFILE
DBCC FREEPROCCACHE	DBCC UPDATEUSAGE

Команды UPDATE STATISTICS и RECOMPILE

Высокая производительность системы SQL Server в значительной степени обеспечивается за счет интеллектуальных процессов обработки сохраняемых в таблицах данных. Необходимый анализ информации осуществляется различными методами, однако самым рациональным из них является изучение сохраняемых в системе реальных данных с целью определения оптимальных путей доступа к ним.

Чтобы лучше уяснить, о чем идет речь, давайте в качестве примера рассмотрим маршрут следования к вашему собственному дому. Весьма вероятно, что вы уже нашли самый оптимальный и быстрый путь между местом работы и местом жительства. И раз этот маршрут уже найден, то чаще всего вы будете пользоваться именно им, даже если кто-то предложит вам воспользоваться иным путем. Ведь вы уже потратили достаточно времени на анализ различных возможных маршрутов и выбрали из них самый оптимальный.

Для того чтобы в сложившийся маршрут были внесены изменения, необходимы достаточно серьезные причины. Это может быть новая дорога, реконструкция уже существующих путей или что-либо в этом роде, способное оказать влияние на время, за которое вы добираетесь домой.

В системе SQL Server подобная аналогия вполне справедлива. При создании хранимой процедуры SQL Server анализирует логику ее оператора SELECT совместно с любыми прочими условиями, зависящими от обрабатываемых данных. На основе этого анализа выбирается оптимальный маршрут обращения к данным при выполнении хранимой процедуры. После того как маршрут определен, информация о нем запоминается, поэтому при каждом следующем выполнении хранимой процедуры используемый в ней алгоритм доступа к данным будет оптимальным. "Маршруты" к данным в SQL Server прокладываются на основе существующих в системе индексов таблиц. Именно эти элементы анализирует система, определяя наиболее эффективный способ доступа к требуемой информации.

Если в процессе работы в таблицу будет добавлено достаточно большое количество строк данных (превышающее 20% ее исходного размера), следует выполнить обновление статистических данных об этой таблице. Используемая для этой цели команда имеет следующий синтаксис:

```
UPDATE STATISTICS table | view
    [
        {
            { index | statistics_name }
          | ( { index |statistics_name } [ ,...n ] )
                }
    ]
    [    WITH
        [
            [ FULLSCAN ]
            | SAMPLE number { PERCENT | ROWS } ]
            | RESAMPLE
            | <update_stats_stream_option> [ ,...n ]
        ]
        [ [ , ] [ ALL | COLUMNS | INDEX ]
        [ [ , ] NORECOMPUTE ]
    ] ;
<update_stats_stream_option> ::=
    [ STATS_STREAM = stats_stream ]
    [ ROWCOUNT = numeric_constant ]
    [ PAGECOUNT = numeric contant ]
```

В команде можно потребовать выполнить пересчет статистики как для одного определенного индекса или столбца данных, так и для всей таблицы в целом. Если указывается отдельный индекс или столбец данных, то это делается так, как показано выше, с одновременным указанием имени таблицы, в которой этот индекс или столбец располагается.

Периодически SQL Server по собственной инициативе использует промежутки времени, когда процессор простаивает, для обработки таблиц с целью поддержания актуальности статистических данных, что способствует повышению эффективности обработки информации в системе.

Режим ручного обновления статистики также сохранен, причем соответствующая команда дополнена новыми параметрами. Так, при указании в команде обновления статистики параметра FULLSCAN SQL Server выполнит полное сканирование указанного индекса или таблицы. Наличие в команде параметра SAMPLE потребует от SQL Server использовать технологию выборок данных на основе указанного количества или процента строк. В этом случае SQL Server должен будет убедиться, что в качестве образца выбрано статистически значимое число значений. Если указанное число или процент строк недостаточно велики для выполнения этого требования, система

автоматически увеличит заданное значение. Последний из параметров INDEX, COLUMN или ALL указывает, для каких объектов должна собираться статистика – индексов, столбцов или и тех, и других. При опускании этого параметра статистика собирается только для индексов.

Для прекращения автоматического сбора статистики (хотя я и не знаю, зачем это может кому-либо потребоваться) следует ввести команду UPDATE STATISTICS с параметром NORECOMPUTE. Указание этого параметра блокирует выполнение процедур автоматического сбора статистики в системе SQL Server.

Статистика по определенной таблице, индексу или столбцу может быть удалена, для чего предназначена команда DROP STATISTICS, имеющая приведенный ниже синтаксис:

DROP STATISTICS таблица.столбец [,...таблица.столбец]

Последним шагом на пути обновления индексов с целью использования новых статистических данных в хранимых процедурах является уведомление SQL Server о необходимости пересчитать маршруты, используемые для извлечения информации из базы данных. Это достигается посредством перекомпиляции хранимых процедур, работающих с данными, статистические сведения о которых были обновлены только что выполненными командами UPDATE STATISTICS.

Обычно хранимые процедуры компилируются в момент первого их вызова после перезапуска системы SQL Server. Существуют и другие ситуации, в которых выполняется автоматическая перекомпиляция хранимых процедур, однако простая выдача команды UPDATE STATISTICS к ним не относится. В качестве примера можно указать ситуацию, когда ликвидируется индекс, ранее использовавшийся в некоторой хранимой процедуре. Иногда можно заметить, что при первом вызове некоторой хранимой процедуры время реакции системы оказывается существенно большим, чем обычно. Причем все последующие вызовы этой процедуры выполняются уже с нормальной скоростью. Это происходит по той причине, что оптимизатор выполнил перекомпиляцию хранимой процедуры с целью учета новых статистических данных, полученных для используемых в запросе таблиц или индексов.

Чтобы перекомпилировать хранимые процедуры, необходимо установить для таблицы соответствующий флажок, предназначенный для извещения системы о том, что любые работающие с этой таблицей и находящиеся в процедурном кэше копии хранимых процедур следует считать недействительными. В результате SQL Server перезагрузит и перекомпилирует все соответствующие процедуры при первом же их вызове. Для установки данного флажка используется следующая команда:

sp_recompile <*имя_таблицы*>

Здесь параметр *имя_таблицы* определяет имя той таблицы, для которой следует перекомпилировать все обращающиеся к ней хранимые процедуры. В случае успешного выполнения команда выводит простое сообщение, уведомляющее, что все связанные с указанной таблицей хранимые процедуры будут перезагружены и перекомпилированы.

Пример:

```
EXEC  sp_recompile  'authors'
GO
```

Результат:

```
Object   'authors'   was  successfully marked for recompilation.
```

Если не перекомпилировать те хранимые процедуры, которые связаны с результатами выполнения команды update statistics, to ожидаемое улучшение производительности достигнуто не будет вплоть до очередной остановки и перезагрузки сервера. Только в этом случае все хранимые процедуры будут автоматически заново перекомпилированы.

Выполнение команд UPDATE STATISTICS и RECOMPILE не может нанести системе никакого вреда, однако делать это рекомендуется в то время, когда активность пользователей в системе относительно невысока. Особенно важно придерживаться этого правила при работе с крупными базами данных. Время, которое будет затрачено на получение новых статистических данных, может существенно отразиться на производительности системы по обработке запросов пользователей. Лучше всего выполнять процедуры обновления статистики как часть регулярных манипуляций, связанных с плановым обслуживанием системы. Например, имеет смысл выполнять эту процедуру не реже, чем раз в месяц для каждой из интенсивно используемых в системе таблиц с невысоким уровнем изменения данных. В случае, когда система только запускается в работу и производится интенсивное заполнение данными ее таблиц, может потребоваться выполнять процедуры обновления статистики гораздо чаще – возможно, даже ежедневно, – если поток новых данных достаточно велик.

Лабораторная работа 14. Консоль управления MMC

Консоль MMC (Microsoft Management Console) — основное средство администрирования в Windows Server 2003. Консоль MMC предоставляет стандартный интерфейс для одного или нескольких приложений, называемых *оснастками* (snap-in), которые применяются для конфигурирования элементов вашей среды. Эти оснастки приспособлены для решения конкретных задач, их можно упорядочивать и группировать в рамках консоли MMC согласно вашим предпочтениям.

Например, преднастроенная консоль *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) разработана специально для администрирования участников безопасности (пользователей, групп и компьютеров) в домене. Консоли в рамках MMC (но не сама MMC) — это и есть используемые вами средства администрирования.

Консоль MMC

Консоль управления MMC — подобие *Проводника Windows,* только с меньшим количеством кнопок. Функциональные компоненты MMC содержатся в так называемых оснастках: меню и панель инструментов предоставляют команды для управления родительскими и дочерними окнами, а сама консоль (состоящая из оснасток) определяет требуемую функциональность. Помимо этого, в зависимости от ситуации консоль MMC можно сохранять с различными параметрами и в разных режимах.

Примечание Консоли MMC работают под управлением Windows Server 2003, Windows 2000/NT 4/ XP/98.

Навигация в консоли MMC

Пустая консоль управления MMC показана на рисунке 6. Заметьте, что ей присвоено имя, и у нее есть узел **Корень консоли (Console Root).**Именно в этот корень консоли будут помещаться все необходимые оснастки.

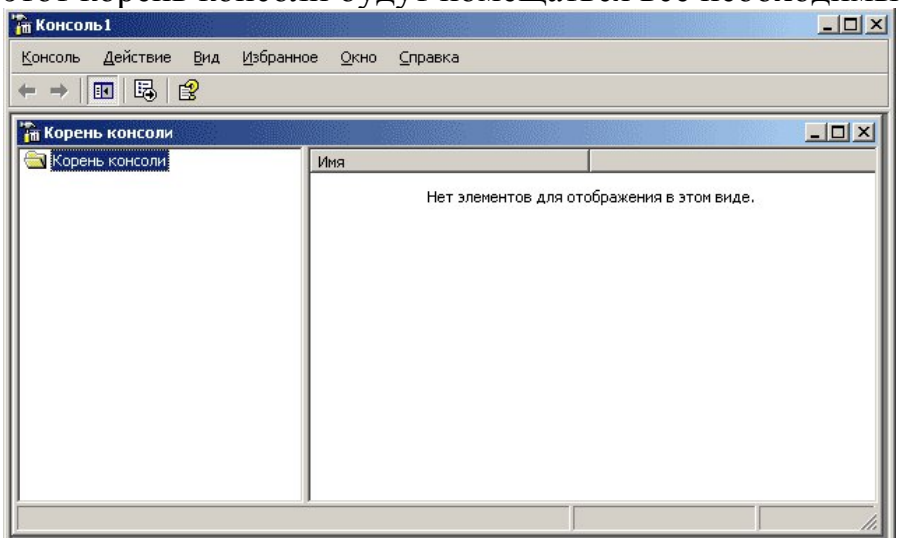

Рисунок 6 - Пустая консоль MMC

В каждой консоли имеется дерево (отображается слева), меню и панели инструментов, а также панель подробных сведений (отображается справа). Содержимое этих элементов зависит от назначения и функциональных

возможностей используемой консоли. На рисунке 7 показана консоль MMC с двумя загруженными оснастками, а также дочерним окном оснастки *Диспетчер устройств* (Device Manager).

Работа с меню и панелью инструментов консоли MMC

Хотя каждая оснастка добавляет собственные уникальные элементы в меню и на панель инструментов, есть несколько ключевых меню и команд, используемых во многих ситуациях и типичных для большинства оснасток (таблица 1).

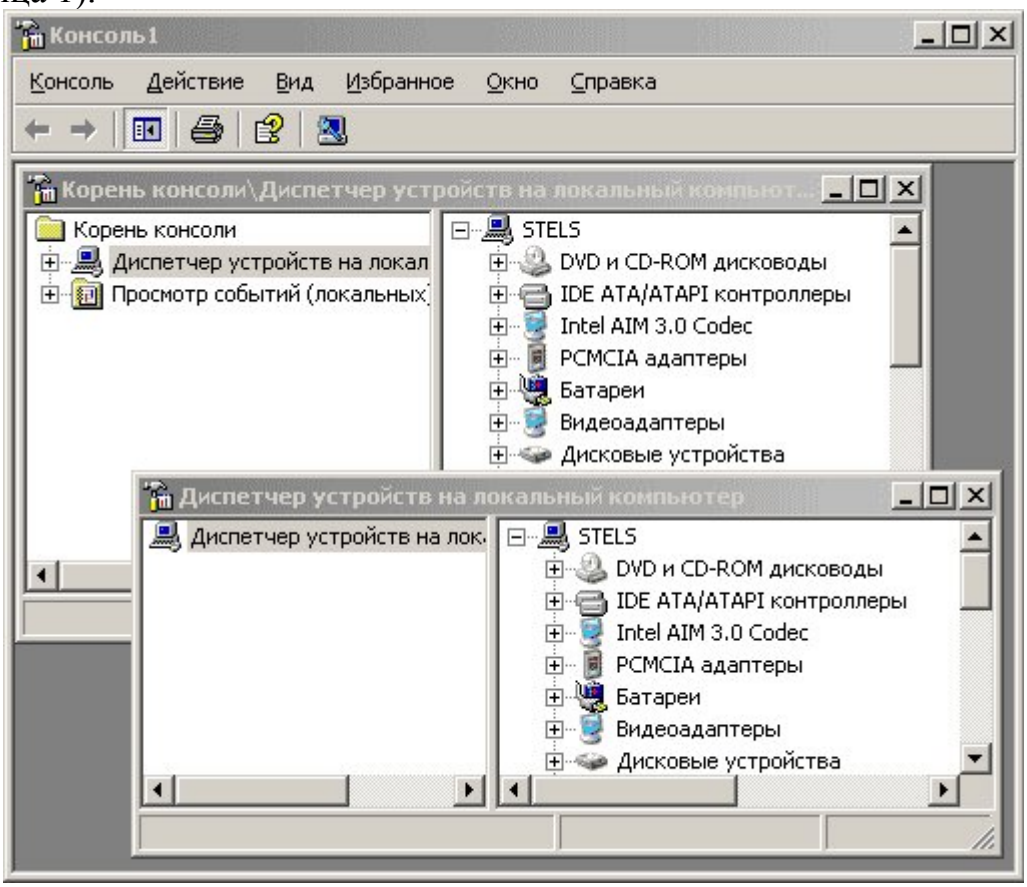

Рисунок 7- Заполненная консоль MMC

Таблица 1 - Типичные меню и команды консоли MMC

Меню	**Команды**
Консоль (Console)	Создание новой и открытие существующей консоли, добавление и удаление оснасток, настройка параметров сохранения консоли, список последних открывавшихся файлов консоли, а также команда выхода
Действие (Action)	Набор команд зависит от оснастки, но обычно включает функции экспорта, вывода, конфигурирования и справки, характерные для данной оснастки
Вид (View)	Набор команд зависит от оснастки, но обычно включает параметры дпя изменения общих характеристик отображения консоли
Избранное (Favorites)	Добавление и организация сохраненных консолей

Окно (Window)	Открытие нового окна, размещение внутренних окон каскадом или сверху вниз, а также переключение между открытыми дочерними окнами данной консоли
Справка (Help)	Стандартное справочное меню консоли MMC, а также модули справки загруженных оснасток

Создание собственной консоли MMC

Каждая консоль содержит набор из одной или нескольких *оснасток* (snap - in), которые расширяют возможности консоли, добавляя функции управления, специфичные для какой-либо задачи. Предусмотрено два типа оснасток: изолированные и оснастки-расширения.

Вы можете объединить одну или несколько оснасток либо их составные части для создания собственных консолей MMC, которые в дальнейшем можно использовать для централизации и комбинирования административных задач. Хотя для задач администрирования можно использовать множество преднастроенных консолей, собственные консоли будут лучше удовлетворять вашим потребностям и способствовать стандартизации вашей среды.

Изолированные оснастки

Изолированные оснастки (standalone snap-in) создаются разработчиками административного приложения. Например, все средства администрирования для Windows Server 2003 являются либо консолями с одной оснасткой, либо преднастроенными сочетаниями оснасток, используемыми для решения конкретной категории задач. Например, консоль *Управление компьютером* (Computer Management) — сборник отдельных оснасток для управления компьютером.

Оснастки расширения

Оснастки-расширения (extension snap - in), или просто *расширения,* предназначены для работы совместно с одной или несколькими изолированными оснастками на основе их функциональности. Когда вы добавляете расширение, Windows Server 2003 помещает его в соответствующее место в рамках изолированной оснастки.

Многие оснастки обладают изолированной функциональностью и, помимо этого, способны расширять функциональность других оснасток. Например, оснастка *Просмотр событий* (Event Viewer) отображает журналы событий компьютеров. Если в консоли имеется объект *Управление компьютером* (Computer Management), то оснастка *Просмотр событий* автоматически дополняет все экземпляры этого объекта и предоставляет средства просмотра журнала событий. С другой стороны, оснастка *Просмотр событий* может работать в изолированном режиме, и не отображаться при этом в иерархии дерева ниже узла **Управление компьютером (Computer Management).**

Параметры консоли

Параметры консоли определяют порядок работы MMC: какие узлы в дереве консоли можно открывать, какие оснастки добавлять и какие окна создавать.

Авторский режим

Когда вы сохраняете консоль в авторском режиме (по умолчанию), то получаете полный доступ ко всей функциональности MMC, в том числе вы можете:

- добавлять и удалять оснастки;
- создавать окна;
- создавать панели задач и задачи;
- просматривать узлы дерева консоли;
- изменять параметры консоли;
- сохранять консоль.

Пользовательские режимы

Если вы планируете распространять консоль MMC, реализующую характерные функции, то можете задать требуемый пользовательский режим, а затем сохранить консоль. По умолчанию файлы консоли записываются в папку *Администрирование* (Administrative Tools) в профиле пользователя. В таблице 2 перечислены пользовательские режимы, доступные при сохранении консоли MMC.

Таблица 2- Пользовательские режимы консоли MMC

Тип пользовательского режима	**Описание**
Полный доступ (Full Access)	Позволяет перемещаться по оснасткам, открывать окна и обращаться ко всем узлам дерева консоли
Ограниченный доступ, несколько окон (Limited Access, Multiple, Windows)	Пользователи не вправе открывать новые окна или обращаться к узлам дерева, но могут просматривать в консоли несколько окон
Ограниченный доступ, одно окно (Limited Access, Single Window)	Пользователи не вправе открывать новые окна или обращаться к узлам дерева и могут просматривать в консоли только одно окно

Примечание Консоль MMC сохраняется с расширением.msc. Например, файл консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) назван Dsa.msc (сокращение от Directory Services Administrator.Microsoft Saved Console).

Лабораторная работа. Создание и сохранение консолей

Цель работы: научиться создавать, настраивать и сохранять консоль MMC.

Упражнение. Консоль Просмотр событий

1. Щелкните **Пуск (Start)\Выполнить (Run).**
2. В поле **Открыть (Open)** введите mmc, затем щелкните **ОК.**

3. Разверните окна **Консоль 1 (Console1)** и **Дерево консоли (Console Root).**
4. В меню **Файл (File)** выберите **Параметры (Options),** чтобы узнать, какой режим настроен для консоли.
5. Убедитесь, что в раскрывающемся списке **Режим консоли (Console Mode)** выбрано **Авторский режим (Author mode)**, затем щелкните**ОК.**
6. В меню **Файл (File)** щелкните **Добавить или удалить оснастку (Add/Remove Snap - In).** Откроется диалоговое окно **Добавить или удалить оснастку (Add / Remove Snap - In)** с выбранной вкладкой **Изолированная оснастка (Standalone)**. Заметьте, что консоль пуста.
7. В окне **Добавить или удалить оснастку** щелкните **Добавить (Add)**, чтобы раскрыть окно **Добавить изолированную оснастку (Add Standalone Snap - In).**
8. Выберите оснастку **Просмотр событий (Event Viewer),** затем щелкните **Добавить (Add).** Откроется диалоговое окно **Выбор компьютера (Select Computer),** в котором можно указать, какой компьютер вы хотите администрировать. Вы можете добавить оснастку Просмотр событий для работы с локальным или удаленным компьютером.
9. В окне **Выбор компьютера (Select Computer)** выберите **Локальный компьютер (Local Computer)**, затем щелкните **Готово (Finish).**
10. В окне **Добавить изолированную оснастку (Add Standalone Snap - In)** щелкните **Закрыть (Close),** а затем в окне **Добавить/удалить оснастку (Add/Remove Snap - Ins)** щелкните **ОК.** В дереве консоли появится новый узел — **Просмотр событий (локальных) [Event Viewer (Local)].** Отрегулируйте мышью ширину панели дерева консоли, чтобы увидеть полное имя узла; вы также можете раскрывать любые узлы этой консоли.
11. Самостоятельно добавьте оснастку *Диспетчер устройств на локальный компьютер* [(Device Manager (local)].
12. Сохраните консоль ММС под именем MyEvents .

Лабораторная работа 15. Создание и управление объектами пользователей

Active Directory требует, чтобы перед разрешением доступа к ресурсам проводилась проверка подлинности пользователя на основе его учетной записи, которая содержит имя для входа в систему, пароль и уникальный *идентификатор безопасности* (security identifier, SID). В процессе входа в систему Active Directory проверяет подлинность имени и пароля. После этого подсистема безопасности может создать маркер доступа, представляющий этого пользователя. В маркере доступа содержатся SID учетной записи пользователя и SID всех групп, к которым относится пользователь. При помощи этого маркера можно проверить назначенные пользователю права, в том числе право локально входить в систему, а также разрешить или запретить доступ к ресурсам, защищенным *таблицами управления доступом* (access control list, ACL).

Учетная запись пользователя интегрирована в объект пользователя в Active Directory. В объекте пользователя хранятся не только имя, пароль и SID , но также контактная информация (например номера телефонов и адреса), организационная информация, в том числе должность, прямые подчиненные и руководитель, сведения о членстве в группах и конфигурации, например параметры перемещаемого профиля, служб терминалов, удаленного доступа и удаленного управления. На этом занятии вы узнаете, как объекты пользователей обрабатываются в Active Directory.

Создание объектов пользователей в консоли *Active Directory — пользователи и компьютеры*

Создать объект пользователя можно в консоли *Active Directory — пользователи и компьютеры*. Хотя их можно создавать в домене или в любом из контейнеров по умолчанию, рекомендуется делать это в ОП, чтобы в полной мере задействовать делегирование административных полномочий и объекты групповой политики (ОГП).

Чтобы создать объект пользователя, выберите нужный контейнер, затем в меню **Действие (Action)** щелкните **Создать (New)\Пользователь (User).** (Для этого вы должны быть членом групп *Администраторы предприятия* (Enterprise Admins), *Администраторы домена* (Domain Admins) или *Операторы учета* (Account Operators), либо вам должны быть делегированы административные полномочия. В противном случае команда создания будет недоступна.)

Откроется диалоговое окно **Новый объект — Пользователь (New Object — User)**. На первой странице этого окна необходимо ввести сведения об имени пользователя (таблица 3).

Таблица 3 - Свойства пользователя на первой странице окна *Новый объект — Пользователь*

Свойство	**Описание**
Имя (First Name)	Имя пользователя. Необязательное
Инициалы (Initials)	Инициалы (отчество) пользователя. Необязательное
Фамилия (Last Name)	Фамилия пользователя. Необязательное

Полное имя (Full Name)	Полное имя пользователя. Если вы указали имя или фамилию пользователя, значение этого свойства будет подставлено автоматически. Впрочем, можно изменить предложенное значение. Это обязательное поле. На основе введенного здесь имени генерируется несколько свойств объекта пользователя, в частности CN (обычное имя), DN (различающееся имя), name (имя) и displayName (отображаемое имя). Поскольку значение CN должно быть в контейнере уникальным, введенное здесь имя должно быть уникальным среди остальных объектов в ОП (или другом контейнере), где вы создаете объект пользователя
Имя входа пользователя (User Logon Name)	*Имя участника-пользователя* (user principal name, UPN) состоит из имени пользователя для входа и суффикса UPN, которым по умолчанию является DNS-имя домена, в котором вы создаете объект. Это свойство обязательно, а UPN-имя в целом (в формате имя_для_входа@суффикс_UPN должно быть уникальным в лесу Active Directory Например, UPN-имя может быть таким: someone@ contoso.com. UPN можно использовать для входа в систему Windows 2000/XP или Windows Server 2003
Имя входа пользователя (пред-Windows2000)[User Logon Name (Pre - Windows 2000)]	Это имя используется для входа в систему с клиентов под управлением более ранних версий Windows , например Windows 9x/Me/NT 4 или Windows NT 3.51. Это поле является обязательным и должно быть уникальным в домене

Закончив ввод значений, щелкните **Далее (Next).** На второй странице окна **Новый объект — Пользователь (New Object — User)** необходимо ввести пароль пользователя и установить управляющие флажки учетной записи.

Внимание! Политика учетных записей по умолчанию в домене Windows Server 2003, которая настраивается в ОГП Default Domain Policy, требует задания сложного пароля длиной не менее семи символов. Под сложностью понимается, что в пароле должны применяться символы трех или четырех типов: прописные и строчные буквы, цифры и специальные символы.

При работе с Windows Server 2003 в тестовой или лабораторной среде следует применять те же методики, что и в производственной сети. То есть для создаваемых учетных записей рекомендуется задавать надежные пароли (вам придется запоминать их для упражнений, требующих входа в систему под именами тестовых пользователей).

В таблице 4 перечислены свойства со второй страницы окна **Новый объект — Пользователь (New Object — User).**

Таблица 4 - Свойства пользователя на второй странице окна *Новый объект — Пользователь*

Свойство	**Описание**
Пароль (Password)	Этот пароль будет использоваться для проверки подлинности пользователя. В целях безопасности пароль необходимо задавать всегда. Во время ввода символы будут скрыты
Подтверждение (Confirm Password)	Подтвердите пароль, набрав его еще раз
Требовать смену пароля при следующем входе в систему(User Must Change Password At Next Logon)	Установите этот флажок, если хотите, чтобы пользователь изменил пароль, введенный вами при первом входе в систему. Если вы выбрали **Срок действия пароля не ограничен (Password Never Expires),**изменить значение этого параметра нельзя. При выборе этого параметра флажок исключающего его параметра **Запретить смену пароля пользователем (User Cannot Change Password)** будет автоматически снят
Запретить смену пароля пользователем (User Cannot Change Password)	Установите этот флажок, если одной учетной записью в домене пользуются несколько человек [допустим, учетной записью *Гость* (Guest)] или если необходимо контролировать пароли учетной записи этого пользователя. Обычно этот параметр используется для управления паролями учетных записей служб. Его нельзя выбрать, если вы установили флажок **Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)**
Срок действия пароля не ограничен (Password Never Expires)	Установите этот флажок, если хотите, чтобы срок действия пароля не истекал. При этом флажок**Требовать смену пароля при следующем входе в систему (User Must Change Password At Next Logon)**будет автоматически снят, так как это взаимоисключающие параметры. Обычно используется для управления паролями учетных записей служб
Отключить учетную запись(Account is disabled)	Установите этот флажок для отключения учетной записи пользователя, допустим, при создании объекта для только что нанятого сотрудника, которому пока не требуется входить в сеть

На заметку При создании объектов новых пользователей для каждого из них выбирайте уникальные сложные пароли, не отвечающие какому-либо предсказуемому шаблону. Включите параметр, который заставляет пользователя сменить пароль при следующем входе в систему. Если пользователь не будет входить в сеть долгое время, отключите его учетную запись. Когда пользователю в первый раз потребуется доступ к сети, убедитесь, что его учетная запись включена. Система попросит пользователя задать новый уникальный пароль, известный только ему.

Некоторые из параметров учетных записей, перечисленных в табл. 2, могут противоречить политикам, настроенным в домене. Например, в политике домена по умолчанию хранение паролей с использованием обратимого шифрования выключено. Однако в редких случаях, требующих обратимого шифрования, значение свойства учетной записи **Хранить пароль, используя обратимое шифрование (Store Password UsingReversible Encryption)** для данного объекта пользователя будет иметь приоритет. Также в домене может быть указан максимальный срок действия пароля, или пользователь должен будет изменить пароль при следующем входе в систему. Если объект пользователя настроен так, что срок действия пароля не ограничен, эти настройки перекроют политики домена.

Управление объектами пользователей из консоли *Active Directory — пользователи и компьютеры*

При создании объекта пользователя требуется настроить общие свойства пользователя, в том числе имена для входа и пароль. На самом деле объекты пользователей поддерживают множество различных свойств, которые вы можете в любой момент настроить при помощи консоли*Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Эти свойства упрощают управление объектами и их поиск.

Чтобы настроить свойства объекта пользователя, выберите объект и в контекстном меню или в меню **Действие (Action)** щелкните **Свойства (Properties).** Откроется окно **Свойства (Properties)** для этого объекта пользователя (рисунок 8).

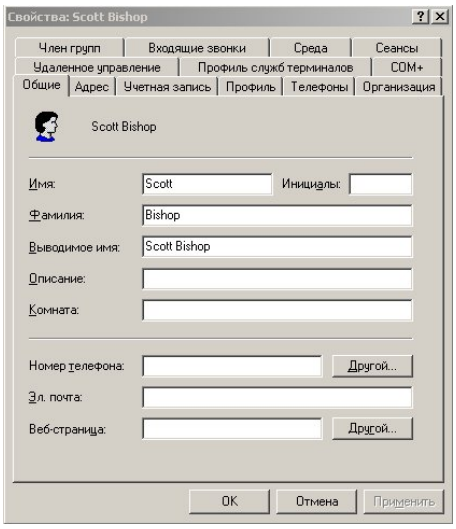

Рисунок 8 - Диалоговое окно *Свойства* для объекта пользователя

Свойства на вкладках этого окна разбиты на несколько основных категорий.

- **Свойства учетной записи: вкладка Учетная запись (Account).** Некоторые из этих свойств настраиваются при создании объекта пользователя, в том числе имена для входа, пароль и управляющие флаги учетной записи.
- **Личная информация: вкладки Общие (General), Адрес (Address), Телефоны (Telephones) и Организация (Organization).** На вкладке**Общие** перечислены свойства учетного имени, которые настраивают при создании объекта пользователя.
- **Управление настройками пользователя: вкладка Профиль (Profile).** Здесь можно указать путь к профилю пользователя, сценарий входа и местоположение домашних папок.
- **Членство в группах: вкладка Член групп (Member Of).** Можно добавить и удалить группы пользователей, а также выбрать основную группу для пользователя.
- **Службы терминалов: вкладки Профиль служб терминалов (Terminal Services Profile), Среда (Environment), Удаленное управление (Remote Control) и Сеансы (Sessions).** Здесь можно настраивать и управлять работой пользователя во время сеанса служб терминалов.
- **Удаленный доступ: вкладка Входящие звонки (Dial - in).** Предназначена для включения и настройки разрешения на удаленный доступ.
- **Приложения: вкладка COM+.** Назначает пользователю наборы разделов Active Directory COM+. Эта новая функция Windows Server 2003 помогает управлять распределенными приложениями.

Свойства учетной записи

Особого внимания заслуживают свойства учетной записи пользователя на вкладке **Учетная запись (Account)** диалогового окна **Свойства (Properties)** пользователя (рисунок 9).

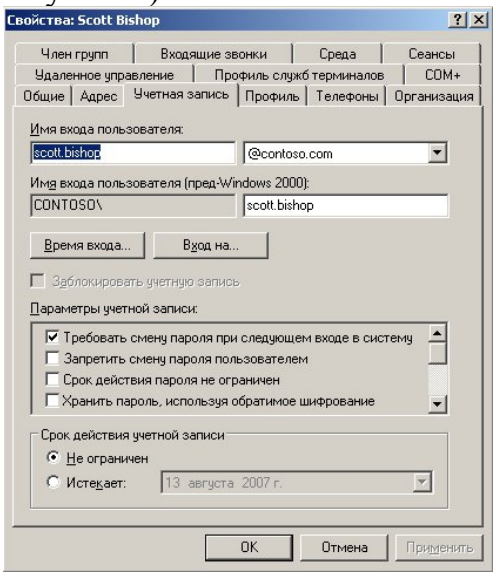

Рисунок 9 - Вкладка *Учетная запись* для объекта пользователя

Некоторые из этих свойств описаны в табл. 3-2. Они были настроены при создании объекта пользователя, и их, как и большой набор других свойств учетной записи, можно изменить на вкладке **Учетная запись (Account).** Значения некоторых свойств не совсем очевидны, они описаны в таблице 5

Таблица 5 - Свойства учетной записи пользователя

Свойство	**Описание**
Время входа (Logon Hours)	Щелкните **Время входа (Logon Hours),** чтобы настроить время, когда пользователю разрешено входить в сеть
Вход на (Log On To)	Щелкните **Вход на (Log On To)**, если хотите запретить пользователю входить в систему с некоторых рабочих станций. В других разделах интерфейса это называется **Ограничения компьютера (ComputerRestrictions).** Чтобы при помоши этой функции ограничивать возможности пользователей, необходимо включить передачу NetBIOS поверх TCP/IP, так как ограничение применяется к имени компьютера, а не к MAC-адресу (Media Access Control) его сетевой платы
Хранить пароль, используя обратимое шифрование (StorePassword Using Reversible Encryption)	Этот параметр, который разрешает хранение пароля в Active Directory без использования мощного алгоритма для необратимого шифрования хешированием, предназначен для поддержки приложений, которым требуется знать пароль пользователя. Если в этом нет крайней необходимости, не включайте этот параметр, так как он существенно ослабляет безопасность пароля. Пароли, которые хранятся с использованием обратимого шифрования, — это практически то же самое, что пароли, записанные открытым текстом. Клиентам Macintosh, которые подключаются по протоколу AppleTalk, необходимо знать пароль пользователя. Если

	пользователь будет входить в систему при помощи клиента Macintosh, необходимо выбрать этот параметр
Для интерактивного входа в сеть нужна смарт-карта (Smart Card Is Required For Interactive Logon)	Смарт-карты — это переносные устройства, защищенные от несанкционированного вмешательства, на которых хранится уникальная идентификационная информация пользователя. Они присоединяются или вставляются в системное устройство и являются дополнительным физическим идентификационным компонентом процесса проверки подлинности
Учетная запись доверена для делегирования (Account Is TrustedFor Delegation)	Этот параметр позволяет учетной записи службы выдавать себя за пользователя, чтобы обращаться к сетевым ресурсам от его имени. Обычно не включается (особенно для объектов, представляющих людей). Чаще он используется для учетных записей служб в трехуровневых (или многоуровневых) инфраструктурах приложений
Срок действия учетной записи (Account Expires)	При помощи управляющих элементов **Срок действия учетной записи (Account Expires)** задается дата окончания действия учетной записи

Одновременное управление свойствами нескольких учетных записей

Windows Server 2003 позволяет одновременно изменять свойства нескольких учетных записей пользователей. Достаточно выбрать несколько объектов пользователей (например, удерживая клавишу Ctrl) и в меню **Действие (Action)** щелкнуть **Свойства (Properties).** Можно выбирать только однотипные объекты, например только пользователей.

Для нескольких объектов пользователей одновременно можно изменить следующие свойства.

- Вкладка **Общие (General):** свойства **Описание (Description), Комната (Office), Номер телефона (Telephone Number), Факс (Fax), Веб-страница (Web Page), Адрес электронной почты (E-mail).**
- Вкладка **Учетная запись (Account):** свойства **Суффикс UPN (UPN Suffix), Время входа (Logon Hours), Вход на (Logon Workstations), Параметры учетной записи (Account Options), Срок действия учетной записи истекает (Account Expires).**

- Вкладка **Адрес (Address):** свойства **Улица (Street), Почтовый ящик (PO Box), Город (City), Штат/Область (State/Province), Почтовый индекс (ZIP/Postal Code), Страна/ Регион (Country/Region).**
- Вкладка **Профиль (Profile):** свойства **Путь к профилю (Profile Path), Сценарий входа (Logon Script)** и **Домашняя папка (Home Folder).**
- Вкладка **Organization (Организация):** свойства **Должность (Title), Отдел (Department), Организация (Company), Руководитель (Manager).**

Остается еще множество свойств, которые для каждого пользователя должны настраиваться отдельно. Кроме того, определенные административные задачи, в том числе изменение паролей и переименование учетных записей, также должны выполняться отдельно для каждого объекта пользователя.

Перемещение объекта пользователя

Если пользователь переводится на другую должность, вам может понадобиться переместить его объект, чтобы отразить изменения в управлении или настройках объекта: выберите его в *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers) и в контекстном меню или в меню **Действие (Action)** щелкните **Переместить (Move).**

Совет Одна из новых возможностей Windows Server 2003 — поддержка в консолях операций перетаскивания (drag-and-drop). Можно перемещать объекты между ОП, просто перетаскивая их в консоли *Active Directory — пользователи и компьютеры.*

Лабораторная работа. Создание и управление объектами пользователей

Цель работы: научиться создавать объекты пользователей и изменять их свойства

Упражнение 1. Создание объектов пользователей

1. Войдите на Server01 как *Администратор* (Administrator).
2. Откройте консоль *Active Directory — пользователи и компьютеры.*
3. Выберите ОП Employees.
4. Создайте учетную запись пользователя со следующей информацией, причем задайте надежный пароль:

Поле	**Введите**
Имя (First Name)	Dan
Фамилия (Last Name)	Holme
Имя входа пользователя (User Logon Name)	Dan.Holme
Имя входа пользователя (пред- Windows 2000) [User Logon Name (Pre-Wmdows 2000)]	Dholme

5. Создайте второй объект пользователя со следующими свойствами:

Поле	**Введите**

Имя (First Name)	Hank
Фамилия (Last Name)	Carbeck
Имя входа пользователя (User Logon Name)	Hank.Carbeck
Имя входа пользователя (пред- Windows 2000) [User Logon Name (Pre-Wmdows 2000)]	Hcarbeck

6. Создайте объект пользователя для себя, следуя тем же соглашениям для имен входа, что и для двух предыдущих объектов.

Упражнение 2. Изменение свойств объекта пользователя

1. Откройте окно **Свойства (Properties)** для вашего объекта пользователя.
2. Задайте подходящие свойства объекта пользователя на вкладках **Общие (General), Адрес (Address), Профиль (Profile), Телефоны (Telephones)** и **Организация (Organization).**
3. Изучите остальные свойства, связанные с вашим объектом пользователя, но пока не изменяйте их.
4. Щелкните **ОК.**

Упражнение 3. Изменение свойств нескольких объектов пользователей

1. Раскройте *Active Directory — пользователи и компьютеры* и перейдите к ОП Employees Contoso.com . Выберите ОП Employees в дереве: справа будут перечислены объекты пользователей, которые вы создали в упражнении 1.
2. Щелкните объект пользователя Dan Holme.
3. Удерживая клавишу Ctrl, щелкните объект пользователя Hank Carbeck.
4. В меню **Дейсгвие (Action)** выберите **Свойства (Properties).**
5. Обратите внимание на различия между появившимся окном и более подробным окном свойств, с которым вы работали в упражнении 2. Изучите свойства, доступные при выборе нескольких объектов, но не изменяйте их.
6. Задайте следующие свойства для двух объектов пользователей:

Вкладка	**Поле**	**Введите**
Общие (General)	**Описание (Description)**	Научил меня всему, что необходимо знать о Windows Server 2003
Общие (General)	**Номер телефона (Telephone Number)**	(425) 555-0175
Общие (General)	**Веб-страница (Web Page)**	http://www.microsoft.com/mspress
Адрес (Address)	**Улица (Street)**	One Microsoft Way
Адрес (Address)	**Город (City)**	Redmond
Адрес (Address)	**Область/край (State/Prov**	Washington

	ince)	
Адрес (Address)	**Почтовый индекс (ZIP/PostalCode)**	98052
Организация(Organization)	**Должность (Title)**	Писатель
Организация(Organization)	**Организация (Company)**	Microsoft Press

7. Щелкните **ОК.**

8. Откройте окно свойств для объекта Dan Holme .

9. Удостоверьтесь, что свойства, которые вы задали на шаге 6, действительно были применены к объекту. Щелкните **ОК.**

10. Щелкните объект пользователя Dan Holme .

11. Удерживая клавишу Ctrl, щелкните объект пользователя Hank Carbeck. Щелкните меню **Действие (Action).**

12. Заметьте: при выборе нескольких объектов пользователей команда **Смена пароля (Reset Password)** недоступна. Какие еще команды недоступны, если выбрано несколько объектов? Поэкспериментируйте, открывая меню **Действие (Action),** когда выбран один или два пользователя.

Лабораторная работа 16. Управление профилями пользователей

Для обеспечения работы пользователей в системе есть элементы, отсутствие которых усложняет жизнь пользователей. Например, если пользователь войдет в систему и не сможет получить доступ к папке **Избранное (Favorites)** в Internet Explorer, или не увидит знакомых ярлыков и документов на рабочем столе, или ему придется заново настраивать словарь, производительность его труда резко снизится, а в службу поддержки поступит звонок. Все эти примеры относятся к компонентам профиля пользователя. Профили можно настраивать, повышая их доступность, безопасность и надежность. На этом занятии вы научитесь управлять локальными, перемещаемыми, групповыми и обязательными профилями пользователей.

Профили пользователей

Профиль пользователя (user profile) — это набор папок и файлов данных, содержащих элементы среды рабочего стола конкретного пользователя. Профиль состоит из:

- ярлыков в меню **Пуск (Start),** на рабочем столе и на панели быстрого запуска;
- документов на рабочем столе и, если не настроена переадресация, в папке **Мои документы (My Documents);**

Совет Свойства папки **Мои** документы (My Documents) и политик перенаправления папок в групповой политике позволяют настраивать хранение папок Мои **документы** в сети. Таким образом, содержимое папки можно хранить на сервере, где ее можно архивировать и проверять на наличие вирусов. Кроме того, вы можете обеспечить пользователю доступ к своей папке, даже если он перейдет на другой компьютер в сети организации. Также папку **Мои документы** можно сделать доступной в автономном режиме, чтобы пользователи могли обращаться к своим файлам локально, без подключения к сети.

- избранных страниц и файлов «cookie» в Internet Explore;
- сертификатов (если они внедрены в сети);
- специальных файлов приложений, например пользовательского словаря, шаблонов и списка автотекста в Microsoft Office;
- содержимого папки **Сетевое окружение (My Network Places);**
- параметров отображения рабочего стола, например его вида, фона и заставки.

Эти важные элементы у каждого пользователя свои. Желательно, чтобы они не изменялись между входами в систему, были доступны, если пользователю потребуется войти в другую систему, и их можно было восстановить в случае, если система даст сбой и ее потребуется переустановить

Локальные профили пользователей

По умолчанию профили пользователей хранятся локально в папке %Systemdrive%\Documents and Settings\%Username% и работают следующим образом.

- Когда пользователь входит в систему впервые, система создает для него профиль путем копирования профиля *Пользователь по умолчанию*(Default User). Имя для нового профиля формируется на основе имени для входа, указанного при первом входе в систему.
- Все изменения рабочего стола пользователя и программной среды хранятся в локальном профиле пользователя. Для каждого пользователя существуют отдельные профили, поэтому все параметры индивидуальны.
- Пользовательская среда расширена за счет профиля *Все пользователи* (All Users), который может включать ярлыки на рабочем столе или в меню **Пуск (Start),** адреса компьютеров в сети и даже данные приложений. Для создания среды пользователя элементы профиля *Все пользователи* (All Users) соединяются с профилем пользователя. По умолчанию только члены группы *Администраторы* (Administrators) могут модифицировать профиль *Все пользователи* (All Users).
- Профиль является локальным в полном смысле. Если пользователь входит в другую систему, документы и параметры, являющиеся частью его профиля, не перемещаются. Вместо этого, когда пользователь впервые входит в систему, она генерирует для него новый локальный профиль.

Перемещаемые профили пользователей

Если пользователь работает на нескольких компьютерах, вы можете настроить *перемещаемый профиль пользователя* (roaming user profile, RUP), чтобы гарантировать сохранность и неизменность его документов и параметров вне зависимости от того, в какую систему он входит. RUP хранит профили на сервере, а значит их можно архивировать, проверять на наличие вирусов и централизованно управлять ими. Даже в среде, где пользователи не перемещаются, RUP обеспечивает сохранность важной информации профиля. Если система пользователя дала сбой и ее необходимо переустановить, RUP гарантирует, что новая пользовательская среда будет идентичная предыдущей.

Чтобы настроить RUP, создайте общую папку на сервере. В идеальном случае это должен быть файловый сервер, на котором часто проводится архивирование.

Примечание Настройте общий доступ так, чтобы всем (Everyone) был разрешен полный контроль над папкой (Full Control). Стандартные разрешения общего доступа в Windows Server 2003 позволяют только чтение (Read) папки, но этого недостаточно для настройки перемещаемого профиля.

На вкладке **Профиль (Profile)** диалогового окна **Свойства (Properties)** пользователя введите **Путь к профилю (Profile Path)** в следующем формате: \\<***имя_сервера***>\<***имя_общего_ресурса*** >\%***Username*****%.**

Вместо переменной %*Usemame*% будет автоматически подставлено имя входа пользователя.

Как видите, это очень просто. При следующем входе система найдет местоположение перемещаемого профиля.

Когда пользователь выходит из системы, его профиль выгружается на сервер профилей. Теперь пользователь может входить в эту или в любую

другую систему в домене, и его документы и настройки, являющиеся частью RUP, всегда будут под рукой.

Примечание Windows Server 2003 представляет новую политику: *Разрешать использование только локальных профилей* Only Allow Local User Profiles). Эта политика, связанная с ОП, содержащим учетные записи компьютеров, не позволяет использовать на данных компьютерах перемещаемые профили. Вместо этого пользователи работают с локальными профилями.

Когда пользователь с RUP впервые входит в новую систему, та не копирует профиль *Пользователь по умолчанию* (Default User), а загружает RUP из сетевого ресурса. Когда пользователь выходит из системы или входит в систему, на которой работал ранее, копируются только измененные файлы.

Создание преднастроенного профиля пользователя

Для упорядочения и предварительной настройки рабочего стола и программной среды можно создавать настроенные профили пользователя, чтобы:

- создать продуктивную рабочую среду с простым доступом к необходимым сетевым ресурсам и приложениям;
- исключить доступ к ненужным ресурсам и приложениям;
- упростить работу службы поддержки по устранению неполадок благодаря более понятному и единообразному рабочему столу.

Для создания преднастроенного профиля пользователя не требуются никакие специальные средства. Просто войдите в систему и измените рабочий стол и настройки приложений по своему усмотрению. Лучше использовать для этого отдельную учетную запись, чтобы без необходимости не изменять собственный профиль.

Создав профиль, войдите в систему с административными реквизитами. Из *Панели управления* раскройте окно **Система (System)**, перейдите на вкладку **Дополнительно (Advanced)** и в области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).** Выберите созданный профиль и щелкните **Копировать (Copy To).** Введите путь к профилю в стандартном формате записи пути (UNC):\\<***имя_сервера***>\<***имя_общего_ресурса***>\<***имя_пользователя***>. В области **Разрешить использование (Permitted To** Use) щелкните **Изменить (Change),** чтобы выбрать пользователя, для которого вы настроили этот профиль. Таблица управления доступом (ACL) для папки профиля будет настроена так, чтобы разрешить доступ этому пользователю. Щелкните **ОК** — профиль будет скопирован из сетевого ресурса.

Примечание Для копирования профиля необходимо быть членом группы *Администраторы* (Administrators).

Теперь раскройте свойства объекта пользователя и на вкладке **Профиль (Profile)** в поле **Путь к профилю (Profile Path)** введите тот же UNC-путь. И все! При следующем входе пользователя в домен этот профиль будет загружен и определит среду пользователя.

Совет Будьте осторожны при использовании преднастроенных (да и всех остальных) перемещаемых профилей, помните о потенциальных проблемах, связанных с различным аппаратным обеспечением систем, на которых может работать пользователь. Например, если ярлыки на рабочем столе организованы под разрешение XGA (1024x768), а пользователь входит в систему с видеоадаптером, который поддерживает только раз решение SVGA (800x600), возможно, некоторые ярлыки не отобразятся.

Также профили не всегда обладают межплатформенной совместимостью. Профиль, созданный для Windows 98, будет неправильно работать в системе Windows Server 2003. Несоответствия будут возникать даже при перемещении между системами Windows Server 2003 и Windows XP или Windows 2000 Professional.

Создание преднастроенного группового профиля

При помощи перемещаемых профилей можно создать стандартную среду рабочего стола для нескольких пользователей с одинаковыми должностными обязанностями. Этот процесс схож с процессом создания преднастроенного профиля для одного пользователя, но результирующий профиль будет доступен нескольким пользователям.

Создайте профиль, выполнив описанные выше действия. При копировании профиля на сервер укажите такой путь: ***<имя_сервера>******<имя_общего_ресурса>******<имя_группового_профиля>.*** Н еобходимо разрешить доступ всем пользователям, которые будут ис пользовать этот профиль. Для этого в области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change)** и выберите группу, в которую входят все пользователи, или группу BUILTIN\USERS, которая включает всех пользователей домена. В действительности профиль будет применен только к тем пользователям, для объектов которых вы указали путь к этому профилю.

После того как профиль скопирован в сеть, необходимо настроить путь к нему для тех пользователей, которым он предназначен. Windows Server 2003 упрощает эту задачу — путь к профилю можно изменить одновременно для нескольких выбранных пользователей. Введите тот же UNC, который вы указали при копировании профиля в сеть, например \\<*имя_сервера*>\<*имя__общего_ресурса*>\<*имя_группового_профил я*>.

Настройка обязательного профиля

Обязательный профиль не позволяет пользователям изменять среду профиля. Точнее, обязательный профиль не сохраняет изменения от сеанса к сеансу. Хотя пользователь и может внести изменения, при следующем входе в систему его рабочий стол будет выглядеть так же, как раньше.

Обязательные профили удобны в ситуациях, когда вы хотите зафиксировать состояние рабочего стола. То есть в практическом смысле обязательные профили полезны, если, создавая групповые профили, вы не хотите, чтобы изменения, которые внесет один пользователь, повлияли на среду других пользователей.

Чтобы сделать профиль обязательным, просто переименуйте файл в корневой папке профиля. Интересно, что обязательные профили не настраиваются путем назначения разрешений. Файл, который вам требуется переименовать, — Ntuser.dat . Это скрытый файл, поэтому убедитесь, что в программе *Свойства папки* (Folder Options) из *Панели управления* вы включили параметр **Показывать скрытые файлы и папки (Showhidden files and folders),** или запустите из командной строки программу attrib, чтобы снять атрибут **Скрытый (Hidden).** Возможно, вам понадобится включить в *Проводнике Windows* отображение расширений файлов.

Найдите файл Ntuser.dat в профиле, который собираетесь сделать обязательным. Переименуйте его в Ntuser.man. Профиль (перемещаемый или локальный) теперь является обязательным.

Лабораторная работа Управление профилями пользователей

Цель работы: научиться создавать и настраивать профили пользователей

Упражнение 1. Настройка объектов пользователей для входа на конт роллер домена

В реальной среде вы вряд ли захотите разрешить пользователям локально входить на контроллер домена, но в нашей тестовой среде с одной системой такая возможность необходима. Существует несколько способов задать необходимое разрешение, но самый простой — добавить группу *Пользователи домена* (Domain Users) в группу *Операторы печати* (Print Operators), которой разрешено входить в систему локально.

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. В дереве выберите контейнер Builtin.
3. Раскройте окно свойств группы *Операторы печати* (Print Operators).
4. На вкладке **Члены группы (Members)** добавьте группу *Пользователи домена* (Domain Users).

Упражнение 2. Создание общего ресурса для профилей

1. На диске C: создайте папку Profiles.
2. Правой кнопкой щелкните папку Profiles и выберите **Общий доступ и безопасность (Sharing and Security).**
3. Перейдите на вкладку **Доступ (Sharing)**.
4. Откройте общий доступ к этой папке, оставив предложенное по умолчанию имя ресурса — Profiles.
5. Щелкните кнопку **Разрешения (Permissions).**
6. Установите флажок **Полный доступ (Full Control).**
7. Щелкните **ОК.**

Внимание! При создании общего ресурса Windows Server 2003 по умолчанию ограничивает к нему доступ. В большинстве организаций для общего ресурса включают разрешение **Полный доступ (Full Control)**, а особые разрешения применяют при помощи свойств на вкладке**Безопасность (Security)**. Впрочем, если администратор не защитил ресурс до того, как открыть к нему общий доступ, Windows Server 2003 в целях безопасности

допускает небольшую ошибку, назначая этому ресурсу доступ только для чтения.

Упражнение 3. Создание шаблона профиля пользователя

1. Создайте учетную запись пользователя, которая будет применяться исключительно для создания шаблонов профилей, по следующим данным:

Поле	**Введите**
Имя (First Name)	Profile
Фамилия (Last Name)	**Учетная запись (Account)**
Имя входа пользователя (User Logon Name)	Profile
Имя входа пользователя (пред-Windows 2000) [User Logon Name (Pre-Windows 2000)]	Profile

2. Завершите сеанс на Server01.
3. Войдите в систему под учетной записью Profile.
4. Настройте рабочий стол, например создайте ярлыки для локальных или сетевых ресурсов, допустим, для системного диска C:.
5. Настройте рабочий стол при помощи приложения *Экран* (Display) из *Панели управления*. На вкладке **Рабочий стол (Desktop)** диалогового окна **Свойства экрана (Display Properties)** можно изменить фон рабочего стола и, щелкнув **Настройка рабочего стола (CustomizeDesktop),** добавить значки **Мои документы (My Documents), Мой компьютер (My Computer), Сетевое окружение (My NetworkPlaces)** и **Internet Explorer.**
6. Завершите сеанс учетной записи Profile.

Упражнение 4. Работа с преднастроенным профилем пользователя

1. Войдите в систему как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система (System).**
3. Перейдите на вкладку **Дополнительно (Advanced).**
4. В области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).** Откроется диалоговое окно **Профили пользователей (User Profiles).**
5. Выберите профиль, который вы настроили для учетной записи Profile.
6. Щелкните **Копировать (Copy To).**
7. В поле **Копировать профиль на (Copy Profile To)** введите \\server01\profiles\hcarbeck.
8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
9. Введите **Hank** и щелкните **ОК.**

10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните **ОК.**
11. После того как профиль будет скопирован в сеть, щелкните **ОК** в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
12. Откройте папку C:\Profiles и убедитесь, что папка профиля Hcarbeck создана.
13. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.
14. Откройте свойства объекта пользователя Hank Carbeck.
15. Перейдите на вкладку **Профиль (Profile).**
16. В поле **Путь к профилю (Profile Path)** введите \\server01\prof iles\%usemame%.
17. Щелкните **Применить (Apply)** и убедитесь, что вместо переменной %*Username*% было подставлено имя hcarbeck. Важно, чтобы путь к профилю соответствовал фактическому сетевому пути к папке профиля.
18. Щелкните **ОК.**
19. Проверьте, что преднастроенный перемещаемый профиль пользователя работает правильно. Для этого выйдите из системы и войдите под именем hank.carbeck@contoso.com. Вы должны увидеть изменения, которые внесли на рабочем столе под учетной записью Profile.

Упражнение 5. Работа с преднастроенным обязательным групповым профилем

1. Войдите в систему как *Администратор* (Administrator).
2. В *Панели управления* дважды щелкните **Система (System).**
3. Перейдите на вкладку **Дополнительно (Advanced).**
4. В области **Профили пользователей (User Profiles)** щелкните **Параметры (Settings).**
5. Выберите профиль, который вы настроили для учетной записи Profile.
6. Щелкните **Копировать (Copy To).**
7. В поле **Копировать профиль на (Copy Profile To)** введите \\server01\profiles\sales.
8. В области **Разрешить использование (Permitted To Use)** щелкните **Изменить (Change).**
9. Введите Users и щелкните **ОК.**
10. Подтвердите значения, введенные в окне **Копирование профиля (Copy To),** и щелкните **ОК.**
11. После того как профиль будет скопирован в сеть, щелкните ОК в окнах **Профили пользователей (User Profiles)** и **Свойства системы (System Properties).**
12. Откройте папку C:\Profiles и убедитесь, что папка профиля Sales создана.
13. В *Панели управления* раскройте **Свойства папки (Folder Options)** и проверьте, что на вкладке **Вид (View)** в области **Дополнительные**

параметры (Advanced Settings) выбран параметр **Показывать скрытые файлы и папки (Show Hidden Files And Folders).**

14. Раскройте папку C:\Profiles\Sales и переименуйте файл Ntuser.dat в Ntuser.man. Этот профиль станет обязательным.
15. В дереве консоли *Active Directory — пользователи и компьютеры* выберите ОП Employees.
16. Выберите в дереве следующие объекты (щелкните первый объект и, удерживая клавишу Ctrl, — остальные): Scott Bishop, Danielle Tiedt, Lorrin Smith Bates.
17. В меню **Действие (Action)** выберите **Свойства (Properties).**
18. Перейдите на вкладку **Профиль (Profile)** и установите флажок **Путь к профилю (Profile Path).**
19. В поле **Путь** к **профилю (Profile Path)** введите \\server01\profiles\sales.
20. Щелкните **ОК.**
21. Проверьте, что преднастроенный перемещаемый профиль пользователя настроен правильно; для этого выйдите из системы и войдите под именем danielle.tiedt@contoso.com.
22. Удостоверьтесь, что профиль обязательный, изменив вид рабочего стола. Вы сможете внести изменения, но они не сохранятся для будущих сеансов.
23. Выйдите из системы и войдите как Danielle Tiedt. Так как профиль обязательный, вы не увидите изменений, сделанных на предыдущем шаге.
24. Выйдите из системы и войдите как Scott Bishop с именем пользователя scott.bishop@contoso.com. Должен появиться рабочий стол без изменений.

Лабораторная работа 17. Понятие типа группы и области действия

Группы (groups) — это контейнеры, содержащие объекты пользователей и компьютеров. Если разрешения безопасности для группы заданы в*таблице управления доступом* (access control list, ACL) для некоего ресурса, то их получают все члены группы.

В Windows Server 2003 существует два типа групп: безопасности и распространения. *Группы безопасности* (security groups) используют для назначения разрешений доступа к сетевым ресурсам. *Группы распространения* (distribution groups) применяются для объединения пользователей в списки рассылки электронной почты. Группу безопасности можно использовать в качестве группы распространения, но не наоборот. Правильное планирование структуры групп влияет на производительность и масштабируемость, особенно в корпоративных средах, содержащих множество доменов.

Совет Хотя в таблицах ACL можно задавать параметры для отдельных участников безопасности (пользователей и компьютеров), эта практика должна быть скорее исключением из общего правила. Если вы обнаружите, что задаете в ACL слишком много исключений для пользователя какой-либо группы, пересмотрите его членство в этой группе.

Функциональные уровни доменов

В Windows Server 2003 доступны четыре функциональных уровня домена: смешанный Windows 2000 (выбирается по умолчанию), основной Windows 2000, промежуточный Windows Server 2003 и основной Windows Server 2003.

- **Смешанный режим Windows 2000.** Поддерживает контроллеры доменов Windows NT 4/2000 и Windows Server 2003.
- **Основной режим Windows 2000.** Поддерживает контроллеры доменов Windows 2000 и Windows Server 2003.
- **Промежуточный режим Windows Server 2003.** Поддерживает контроллеры доменов Windows NT 4 и Windows Server 2003.
- **Windows Server 2003.** Поддерживает контроллеры доменов Windows Server 2003.

Ограничения в отношении свойств групп, обсуждаемые в этой и других главах, будут относиться к этим функциональным уровням доменов.

Область действия группы

Область действия группы (group scope) определяет, каким образом участникам группы назначаются разрешения. В Windows Server 2003 и группы безопасности, и группы распространения классифицируют по трем областям действия: локальная доменная, глобальная и универсальная.

Примечание Хотя локальные группы не классифицируются по области действия Windows Server 2003, они включены для полноты картины.

Локальные группы

Локальные группы (local groups), или локальные группы компьютеров, используются в основном для обратной совместимости с Windows NT 4. На компьютерах с Windows Server 2003 существуют локальные пользователи и

группы, сконфигурированные как рядовые серверы. Контроллеры доменов не используют локальные группы.

- Локальные группы могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.
- Локальная группа действует в пределах конкретного компьютера и может предоставлять разрешения для ресурсов только на этом компьютере.

Локальные группы домена

Локальные группы домена (domain local groups) главным образом используются для назначения глобальным группам разрешений на доступ к локальным ресурсам домена. Характерные черты локальных групп домена таковы.

- Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.
- Доступны в пределах всего домена только в доменах основного режима Windows 2000 или доменах Windows Server 2003. Локальная группа домена функционирует подобно локальной группе на контроллере домена, пока домен работает в смешанном режиме.
- Могут содержать участников из любого домена в пределах леса, из доверенных доменов в других лесах и более низкого уровня.
- Действуют в пределах домена в основном режиме Windows 2000 и режиме Windows Server 2003 и могут использоваться для предоставления прав на ресурсы на любом компьютере с Windows Server 2003 в том домене, где определена группа.

Глобальные группы

Глобальные группы (global groups) чаше используются для предоставления категоризированного членства в локальных группах доменов для отдельных участников безопасности и для прямого назначения разрешений (в частности, в доменах смешанного или промежуточного режимов). Часто глобальные группы применяются для объединения пользователей или компьютеров в одном домене и совместного исполнения одной работы, роли или функции. Характеристики глобальных групп таковы.

- Существуют во всех режимах работы доменов и лесов — смешанном, промежуточном и основном.
- Могут содержать только членов из своего домена.
- Могут сами являться членами локальной группы компьютера или домена.
- Могут получать разрешения в любом домене, включая доверенные домены в других лесах и домены пред- Windows 2003.
- Могут содержать другие глобальные группы, но только в домене, работающем в основном режиме Windows 2000 или в режиме Windows Server 2003.

Универсальные группы

Универсальные группы (universal groups) в основном применяют для предоставления доступа к ресурсам во всех доверенных доменах. Однако такие группы могут использоваться только как участники безопасности (то есть как

группы безопасности) в доменах, работающих в основном режиме Windows 2000 или в режиме Windows Server 2003.

- Универсальные группы могут содержать участников из любого домена в лесу.
- В домене основного режима Windows 2000 или режима Windows Server 2003 универсальным группам могут предоставляться разрешения в любом домене, включая доверенные домены в других лесах.

Совет Универсальные группы помогают представить и объединить группы, которые распределены по разным доменам и выполняют типичные функции в рамках вашей организации. Рекомендуется делать универсальными широко используемые и редко изменяемые группы.

Преобразование групп

Область действия группы определяется в момент ее создания. Однако в домене основного режима Windows 2000 или режима Windows Server 2003 локальные группы домена и глобальные группы можно преобразовать в универсальные, если исходные группы не участвуют в других группах с той же областью действия. Например, глобальную группу, входящую в состав другой глобальной группы, нельзя преобразовать в универсальную. Варианты использования доменных групп Windows Server 2003 в качестве участников безопасности приведены в таблице 8 (тип: группа безопасности).

Таблица 8 - Область действия групп и допустимые объекты

Область действия группы	Допустимые объекты
Домен основного режима Windows 2000 или режима Windows Server 2003	
Локальная группа домена	Учетные записи компьютеров, пользователи, глобальные группы и универсальные группы из любого леса или доверенного домена. Локальные группы домена из того же домена. Вложенные локальные группы домена из того же домена
Глобальные группы	Пользователи, компьютеры и глобальные группы из того же домена. Вложенные глобальные группы (из того же домена), локальные группы домена или универсальные группы
Универсальные группы	Универсальные группы, глобальные группы, пользователи и компьютеры из любого домена в лесу. Вложенные глобальные группы, локальные группы домена или универсальные группы
Домен смешанного режима Windows 2000 или промежуточного режима Windows Server 2003	
Локальная группа домена	Учетные записи компьютеров, пользователи, глобальные группы из любого домена. Не могут быть вложенными
Глобальные группы	Только пользователи и компьютеры из того же домена. Не могут быть вложенными
Универсальные группы	Недоступны

Специальные группы

Существует также несколько *специальных групп* (special identity), которые управляются самой ОС. Их нельзя создать, удалить или изменить их состав. Специальные группы не отображаются в консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и другими средствами управления компьютером, однако им можно назначить разрешения в ACL ресурса. Некоторые специальные группы Windows Server 2003 (их также называют особыми) перечислены в таблице 9.

Таблица 9 - Специальные группы и их представление

Специальная группа	Представление
Все (Everyone)	Представляет всех пользователей сети, в том числе вошедших под гостевой учетной записью, а также пользователей из других доменов. Каждый раз при входе в систему пользователь автоматически добавляется в группу *Все* (Everyone)
Сеть (Network)	Представляет пользователей, которые в настоящий момент обращаются к данному ресурсу по сети (в отличие от тех, кто обращается к ресурсу локально). При любом обращении к данному ресурсу по сети пользователь автоматически добавляется в группу *Сеть* (Network)
Интерактивные (Interactive)	Представляет всех пользователей, которые локально обращаются к ресурсу (в отличие от тех, что обращаются к ресурсу по сети). При любом обращении к данному ресурсу пользователь автоматически добавляется в группу *Интерактивные* (Interactive)
Анонимный вход (Anonymous Logon)	В эту группу зачисляются те, кто использует сетевые ресурсы, не пройдя проверку подлинности
Прошедшие проверку(Authenticated Users)	В эту группу входят все пользователи, которые прошли проверку подлинности при входе в сеть, предоставив действительную учетную запись. При назначении разрешений можно вместо *Все* (Everyone) использовать группу *Прошедшие проверку* (Authenticated Users), чтобы избежать анонимного доступа к ресурсам
Создатель-владелец (Creator Owner)	В эту группу зачисляется пользователь, который создал ресурс или получил право владения им. Например, если пользователь создал ресурс, но *Администратор* (Administrator) получил право владения им, в группе*Создатель-владелец* (Creator Owner) будет указан *Администратор*
Удаленный доступ (Dialup)	В группу *Удаленный доступ* (Dialup) зачисляют всех, кто подключен к сети через коммутируемое соединение

Внимание! Этим группам можно назначить разрешения на сетевые ресурсы, однако соблюдайте при этом осторожность. Члены этих групп могут не всегда проходить проверку подлинности в домене. Например, если вы предоставите все права на общий ресурс группе *Все* (Everyone), пользователи, подключающиеся из других доменов, также получат доступ к этому ресурсу.

Упражнение. Создание и изменение группы

В этом упражнении вы измените тип группы и ее область действия.

1. В консоли *Active Directory — пользователи и компьютеры* раскройте контейнер Users и создайте в нем глобальную группу распространения Agents.
2. Щелкните правой кнопкой группу Agents и выберите Свойства (Properties). Можете ли вы изменить область действия и тип этой группы? Почему?

   Если вы не можете изменить тип и область действия группы, ваш домен работает в смешанном режиме Windows 2000 или в промежуточном режиме Windows Server 2003. Чтобы изменить тип или область действия группы, необходимо перевести домен в основной режим Windows 2000 или в режим Windows Server 2003.

Лабораторная работа 18. Управление учетными записями групп

Консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) является основным средством, которое вы будете использовать для управления объектами (пользователями, группами и компьютерами) в домене. При создании групп вы будете указывать область действия, тип и состав. Также с помошью этой консоли вы сможете изменить состав существующих групп.

Создание группы безопасности

Обычно группы создают из консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers), ярлык которой расположен в группе программ **Администрирование (Administrative Tools)**. В окне консоли щелкните правой кнопкой в правой панели контейнера, где вы хотите создать группу, и выберите **Создать (New)\Группа (Group)**. Затем определите тип и область действия создаваемой группы.

Чаще всего вы будете создавать группы безопасности, поскольку им можно назначать разрешения в ACL. В домене смешанного или промежуточного режима группа безопасности может быть только глобальной или локальной группой домена. В таком домене нельзя создать группу безопасности с универсальной областью действия (рисунок 10).

Впрочем, локальную группу домена, глобальную или универсальную группу в доменах смешанного или промежуточного режима можно создать в виде группы распространения. Группы безопасности в таком домене могут иметь локальную доменную или глобальную область действия.

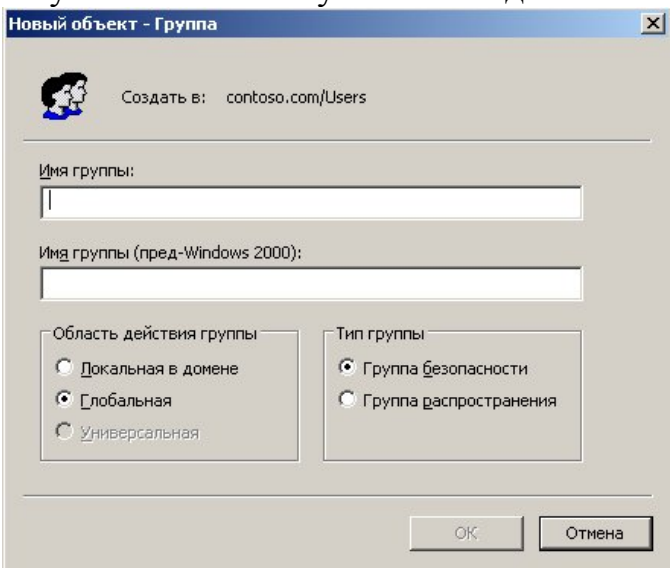

Рисунок 10 - Группы безопасности в доменах смешанного или промежуточного режима

Изменение состава группы

Добавление или удаление членов группы также выполняется из консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers). Щелкните правой кнопкой любую группу и выберите **Свойства (Properties).** На рисунке 11 показано окно свойств для глобальной группы безопасности Sales.

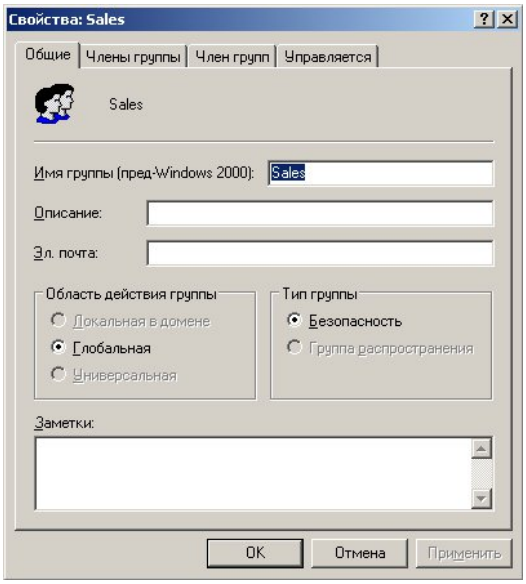

Рисунок 11 - Окно свойств группы безопасности Sales

В таблице 10 описаны вкладки этого окна свойств для настройки членства.

Таблица 10 - Настройка членства

Вкладка	Назначение
Члены группы (Members)	Добавление, удаление и отображение списка участников безопасности — членов этого контейнера
Член групп (Member Of)	Добавление, удаление и отображение перечня контейнеров, членом которых является данный контейнер

Лабораторная работа 19. Присоединение компьютера к домену

В стандартной конфигурации Windows Server 2003 и всех ОС Microsoft Windows компьютер принадлежит какой-либо *рабочей группе* (workgroup). В рабочей группе компьютер на базе Windows NT (включая Windows NT 4, 2000, XP и Windows Server 2003) может проверять подлинность пользователей только из своей локальной БД *диспетчера учетных записей безопасности* (Security Accounts Manager, SAM). Такая система автономна во всех смыслах. Принадлежность к рабочей группе позволяет лишь видеть список компьютеров своей группы в *Проводнике.* Хотя пользователь такого компьютера и может подсоединяться к общим ресурсам на других машинах в рабочих группах или доменах, он на самом деле не входит в систему под доменной учетной записью.

Чтобы пользователь входил в систему под доменной учетной записью, компьютер должен принадлежать какому-нибудь домену: необходимо создать учетную запись компьютера и настроить его для присоединения к домену по этой учетной записи, чему и посвящено это занятие.

Учетная запись компьютера, как и учетная запись пользователя, содержит имя, пароль и *идентификатор безопасности* (security identifier, SID). Эти свойства встроены в класс объекта компьютера в Active Directory. Подготовка к включению компьютера в домен, таким образом, очень похожа на подготовку объекта пользователя для добавления в домен: вам нужно создать в Active Directory объект компьютера.

Создание учетных записей компьютеров

Для создания объекта компьютера в Active Directory необходимо быть членом групп *Администраторы* (Administrators) или *Операторы учета* (Account Operators) на контроллерах домена. Члены групп *Администраторы домена* (Domain Admins) и *Администраторы предприятия* (Enterprise Admins) по умолчанию являются участниками группы *Администраторы* (Administrators). Также можно делегировать административные права, чтобы другие пользователи или группы могли создавать объекты компьютеров.

Впрочем, пользователи домена также могут создавать объекты компьютеров косвенным путем. Когда компьютер присоединяется к домену, а учетная запись еще не создана, Active Directory по умолчанию автоматически создает объект компьютера в контейнере Computers. Каждому пользователю из группы *Прошедшие проверку* (Authenticated Users) (то есть всем пользователям) разрешается присоединять к домену до 10 компьютеров и, следовательно, создавать до 10 объектов компьютеров.

Создание объектов компьютеров в консоли *Active Directory — пользователи и компьютеры*

Чтобы создать объект компьютера, или его учетную запись, откройте консоль *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) и выберите контейнер или ОП, в котором нужно создать объект. В меню **Действие (Action)** или в контекстном меню выберите команду **Создать (New)\Компьютер (Computer).** Откроется диалоговое окно **Новый объект — Компьютер (New Object — Computer),** показанное на рисунке 12.

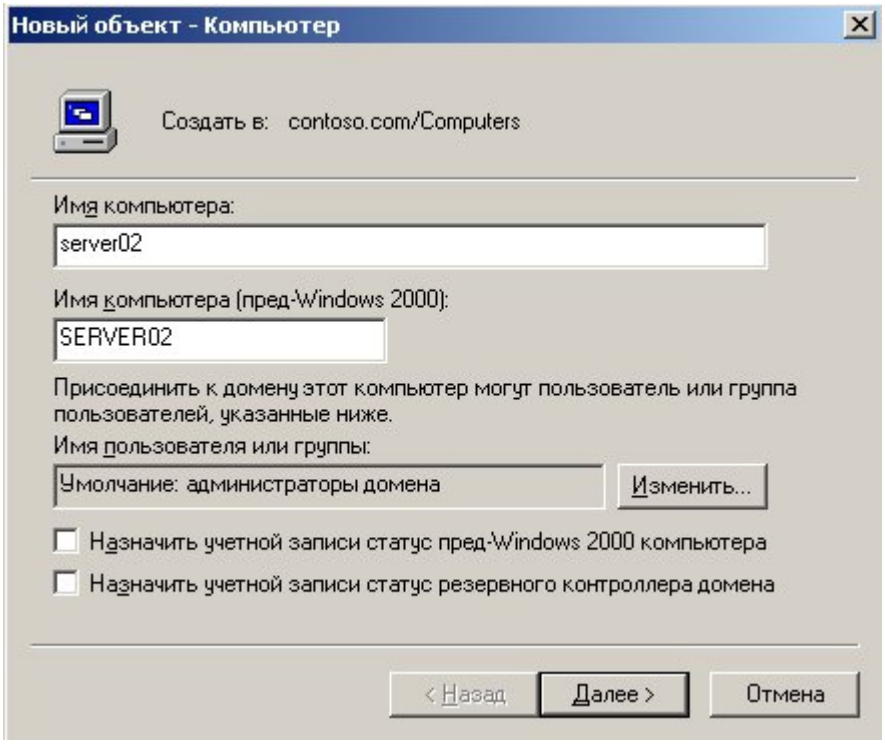

Рисунок 12 - Диалоговое **окно** *Новый объект — **Компьютер***

В окне **Новый объект — Компьютер (New Object — Computer)** введите имя компьютера. Другие свойства из этого окна обсуждаются на следующем занятии. Щелкните **Далее (Next).** На следующем шаге запрашивается глобально уникальный идентификатор (GUID). GUID используется для предварительной настройки учетной записи компьютера для развертывания системы с помощью *служб удаленной установки* (Remote Installation Services, RIS). Здесь этот процесс не обсуждается. При создании учетной записи компьютера, который будет присоединяться к домену другими способами, вводить GUID не требуется. Поэтому просто щелкните **Далее (Next),** а затем **Готово (Finish).**

Присоединение компьютера к домену

Собственно учетной записи компьютера недостаточно для создания необходимых безопасных отношений между доменом и компьютером. Компьютер нужно присоединить к домену.

1. Щелкните правой кнопкой **Мой компьютер (My Computer)** и выберите **Свойства (Properties).** Перейдите на вкладку **Имя компьютера (Computer Name).**
    - В *Панели управления* выберите **Система (System)** и в диалоговом окне **Свойства системы (System Properties)** перейдите на вкладку **Имя компьютера (Computer Name).**
    - Откройте окно свойств **Имя компьютера (Computer Name).** К свойствам компьютера на этой вкладке можно получить доступ несколькими способами.

Примечание В Windows 2000 вкладка **Имя компьютера (Computer Name)** называется **Сетевая идентификация (Network Identification),** а кнопка

Изменить (Change) — Свойства (Properties). Тем не менее, работают они одинаково.

2. В *Панели управления* откройте **Сетевые подключения (Network Connections)** и в меню **Дополнительно (Advanced)** выберите Сетевая **идентификация (Network Identification).**
3. На вкладке **Имя компьютера (Computer Name)** щелкните кнопку **Изменить (Change).** Диалоговое окно **Изменение имени компьютера (Computer Name Changes)** позволяет изменить имя компьютера и его принадлежность к домену и рабочей группе (рис. 5-2).

Примечание Нельзя изменять имя компьютера или его членство, если вы вошли в систему не с администраторскими реквизитами. Кнопка **Изменить (Change)** доступна только пользователям из локальной группы *Администраторы* (Administrators).

4. В окне **Изменение имени компьютера (Computer Name Changes)** установите переключатель в положение **домена (Domain)** и введите нужное имя домена.

Совет Хотя нужный домен обычно можно найти по «плоскому» NetBIOS-имени, возьмите за правило вводить DNS-имя целевого домена. Конфигурация DNS жизненно важна для компьютера с Windows 2000/XP или Windows Server 2003. Используя для домена DNS-имя, вы активизируете предпочтительный процесс разрешения имен и проверяете конфигурацию DNS на данном компьютере. Если компьютер не сможет найти домен, к которому вы пытаетесь присоединить его, проверьте правильность параметров DNS-сервера, заданных в свойствах сетевого подключения.

5. Щелкните ОК. Компьютер попытается связаться с контроллером домена. Если связаться с доменом не удается, проверьте сетевые подключения и их параметры, а также конфигурацию DNS.

Когда компьютер успешно свяжется с доменом, появится приглашение (рис. 5-3) для ввода имени пользователя и пароля, у которого есть привилегии присоединять компьютер к домену. Заметьте: запрошенные имя и пароль — это доменное имя и пароль.

Если в домене заранее не была создана учетная запись компьютера с тем же именем, по умолчанию Active Directory автоматически создаст такую учетную запись в контейнере Computers. После того как доменная учетная запись компьютера найдена или создана, компьютер установит доверительные отношения с доменом, изменит свой SID, чтобы он совпадал с SID этой доменной учетной записи, и изменит свое членство в группах. Для завершения процесса компьютер необходимо перезагрузить.

Примечание: Для присоединения рабочей станции или сервера к домену также можно применять команду NETDOM JOIN. Ее функции идентичны возможностям диалогового окна **Изменение имени компьютера (Computer Name Changes),** но она позволяет задать еще и ОП, в котором будет создана учетная запись, если соответствующего объекта компьютера еще нет в Active Directory.

Лабораторная работа. Присоединение компьютера к домену Active Directory

Цель работы: научиться создадавать учетные записи компьютеров при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users and Computers); научиться присоединять компьютер к домену.

Упражнение 1. Создание объектов компьютеров в консоли *Active Directory — пользователи и компьютеры*

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. В ОП Servers создайте объект для компьютера с именем SERVER02. Задайте только имя компьютера. Не меняйте значения других параметров по умолчанию. Заметьте, что у компьютера, как и у пользователя, два имени — указанное имя компьютера и имя в формате пред- Windows 2000. На практике лучше, чтобы эти имена оставались одинаковыми.

Упражнение 2. Перемещение объекта компьютера

1. Откройте консоль *Active Directory — пользователи и компьютеры.*
2. Командой **Переместить (Move)** переместите компьютер Desktop03 из ОП Servers в ОП Desktops.
3. Перетащите значок Server02 из контейнера Servers в Computers.
4. Выберите контейнер Computers и убедитесь, что Server02 появился в нужном месте. При перетаскивании объектов можно ошибиться.

На заметку MMC печально известна тем, что может вызвать небольшую панику. Она не обновляет содержимое окна автоматически. После таких изменений, как перемещение объекта, необходимо обновить консоль командой **Обновить (Refresh)** или клавишей F5.

5. Откройте окно свойств для контейнера Computers. Вы увидите, что здесь нет вкладки **Групповая политика (Group Policy),** в отличие от ОП, например Servers. Это одна из причин, почему принято создавать одно или несколько дополнительных ОП для объектов компьютеров.
6. Из командной строки исполните следующую команду:

dsmove ?CN=Server02,CN=Computers,DC=contoso,DC=com? -newparent ?0U=Servers,DOcontoso,DC=com?

Эта команда, как легко догадаться, перемещает объект компьютера обратно в ОП Servers.

7. Проверьте, что этот компьютер снова находится в ОП Servers.

Упражнение 3 (необязательное). Присоединение компьютера к домену

Для этого упражнения необходим второй компьютер, подключенный к Server01. Кроме того, нужно правильно сконфигурировать DNS, чтобы для Server01 была создана запись ресурса службы (SRV). На втором компьютере DNS должна быть сконфигурирована так, чтобы он мог находить Server01 как контроллер домена contoso.com.

1. Если у вас есть второй компьютер, который можно в следующем упражнении присоединить к вашему домену, создайте для него учетную запись в ОП Desktops при помощи консоли *Active Directory — пользователи и компьютеры* (Active Directory Users And Computers) или

команды DSADD. Убедитесь, что используемое вами имя совпадает с именем этого компьютера.

2. Войдите в систему на этом компьютере. Чтобы изменять членство этого компьютера в доменах, нужно войти в систему под учетной записью локальной группы *Администраторы* (Administrators).
3. Откройте вкладку **Имя компьютера (Computer Name).** Для этого дважды щелкните **Система (System)** в *Панели управления* или в папке **Сетевые подключения (Network Connections),** в меню **Дополнительно (Advanced)** выберите **Сетевая идентификация (Network Identification).**
4. Щелкните **Изменить (Change).**
5. Установите переключатель в положение **домена (Domain)** и введите DNS-имя домена: contoso.com.
6. Щелкните **ОК.**
7. По запросу введите имя и пароль учетной записи администратора домена contoso.com.
8. Щелкните **ОК.**
9. Вам будет предложено перезагрузить систему. Щелкайте **ОК** в ответ на все сообщения и закройте все диалоговые окна. Перезагрузите систему.

Лабораторная работа 20. Архивация данных

Успех любой процедуры резервного копирования зависит от правильного выбора средств и планирования. В состав Windows Server 2003 входит надежная, гибкая служебная программа Ntbackup. Она поддерживает большинство функций, которые встречаются в средствах сторонних разработчиков, включая возможность составления расписания архивации и взаимодействия со *Службой теневого копирования тома* (Volume Shadow Copy Service, VSS) и системой RSM (Removable Storage Management). На этом занятии вы рассмотрите концептуальные и процедурные вопросы архивации данных и изучите основы планирования и создания заданий резервного копирования с помощью программы Ntbackup.

Знакомство с программой *Архивация данных*

Чтобы запустить программу резервного копирования, часто называемую по имени исполняемого файла — Ntbackup, в меню **Пуск (Start)** выберите **Все программы (All Programs)\Стандартные (Accessories) Служебные (System Tools)\Архивация данных (Backup).** Также ее можно запустить из диалогового окна **Запуск программы (Run)** командой ntbackup.exe.

В первый раз утилита резервного копирования запускается в режиме мастера (рисунок 23). В этой главе обсуждается более распространенный интерфейс программы *Архивация данных.* Если вы, как и большинство администраторов, считаете, что проще использовать стандартный интерфейс, снимите флажок **Всегда запускать в режиме мастера (Always Start In Wizard Mode),** а затем щелкните ссылку **Расширенный режим (Advanced Mode).**

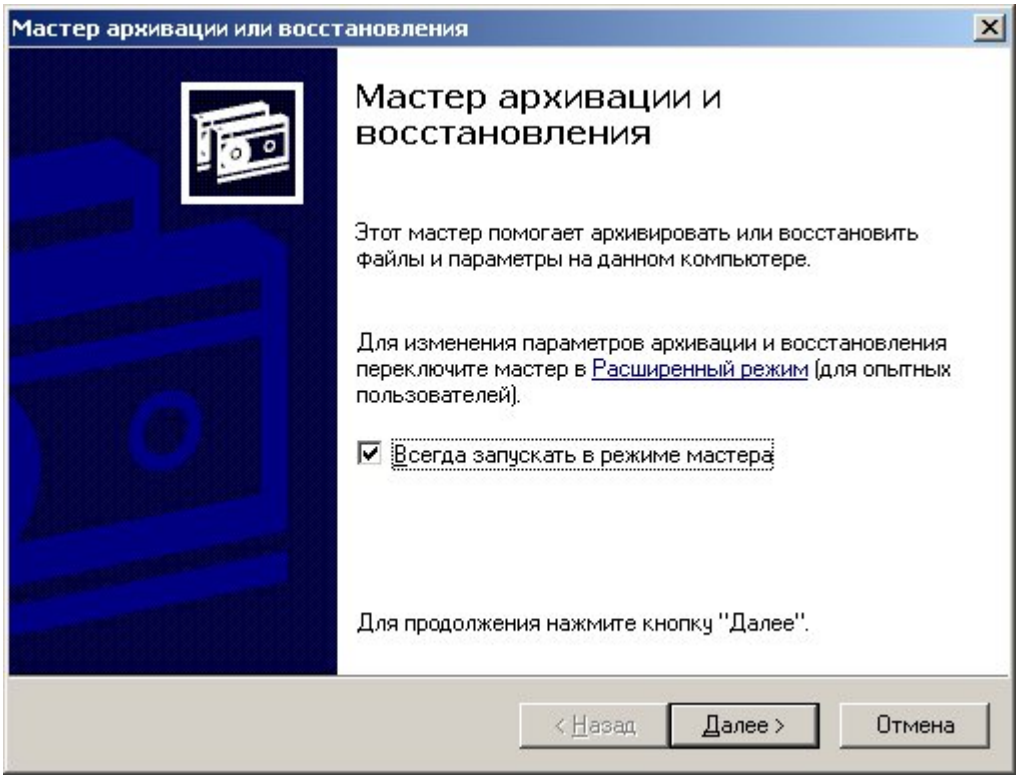

Рисунок 23 - Окно *Мастера архивации и восстановления*

Как видно на вкладке **Добро пожаловать! (Welcome),** резервное копирование можно выполнить вручную, на вкладке **Архивация (Backup),** или с помощью мастера (рисунок 24). Кроме того, можно составить расписание для автоматического выполнения заданий архивации. Программа Backup позволяет также восстанавливать данные вручную, на вкладке **Восстановление и управление носителем (Restore And Manage Media),** или с помощью мастера **Мастер восстановления (Restore).** Далее в этой главе обсуждается мастер ASR (Automated System Recovery), предназначенный для архивации важных файлов ОС.

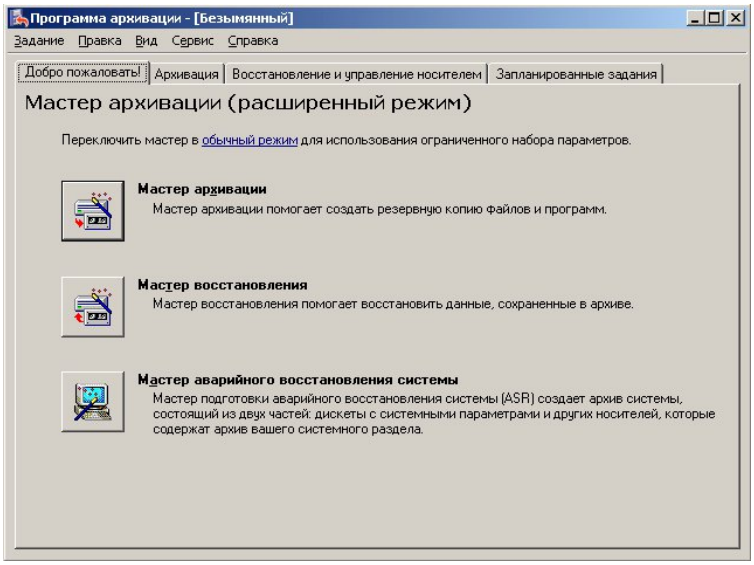

Рисунок 24 - Вкладка *Добро пожаловать!* программы *Архивация данных*

Это занятие посвящено планированию и выполнению архивации данных. Для изучения возможностей программы *Архивация данных* мы будем пользоваться вкладкой **Архивация (Backup),** показанной на рисунке 25.

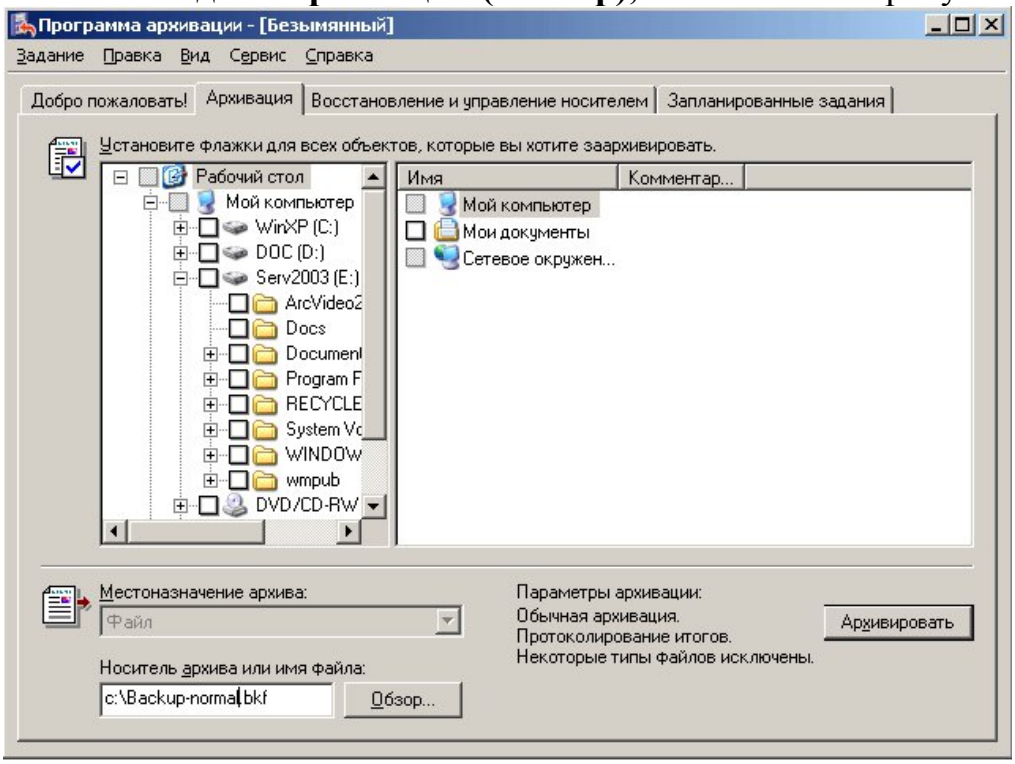

Рисунок 25 - Вкладка *Архивация* программы *Архивация данных*

Выбор файлов для архивации

Вкладка **Архивация (Backup)** позволяет выбрать файлы и папки для архивации. Ресурсы могут находиться на локальных томах или в сетевых папках. Когда папка выбирается целиком, она помечается синим флажком, если же выбираются только некоторые ресурсы — серым (частичная архивация).

Для архивации файлов или папок с удаленного компьютера выберите элементы с сетевого диска или раскройте окно **Сетевое окружение (My Network Places).** Последний способ более трудоемкий (необходимо раскрыть больше уровней, чтобы найти нужные файлы), но и более предпочтительный, поскольку привязки дисков меняются чаще, чем пути UNC.

Выбор носителя архива

Windows Server 2003 позволяет записывать резервные копии на различные типы носителей: магнитную ленту, сменный диск (такой как Iomega Jaz) и, конечно, непосредственно в файл на дисковом томе. При использовании магнитной ленты указанное имя должно совпадать с именем ленты в накопителе.

При архивации в файл программа Backup создает файл с расширением .bkf в указанном размещении (на локальном томе или в удаленной папке). Нередко администраторы архивируют данные на каждом сервере и объединяют файлы архивов на центральном сервере, с которого затем данные записываются на сменный носитель. При таком подходе в качестве размещения архива указывается UNC-путь к папке центрального сервера или к

локальному файлу на каждом сервере; затем этот архив копируется в центральное размещение.

Программа *Архивация данных* имеет два важных ограничения. Во-первых, она не поддерживает перезаписываемые форматы DVD и CD. Чтобы обойти это ограничение, заархивируйте данные в файл, а затем скопируйте его на DVD- или компакт-диск. Во-вторых, архивация в любое размещение (за исключением файла) требует, чтобы носитель находился в устройстве, физически подключенном к системе. Это означает, что вы не сможете создать резервную копию данных на ленточном накопителе, который подсоединен к удаленному серверу.

Определение стратегии архивации

Выбрав файлы для архивации и указав размещение резервной копии, нужно выбрать тип архива, определяющий, какие именно из выбранных файлов будут копироваться на целевой носитель. Щелкните кнопку **Архивировать (Start Backup),** затем **Дополнительно (Advanced)** — откроется окно **Дополнительные параметры архивации (Advanced Backup Options),** позволяющее указать тип архива.

Каждый тип архива так или иначе связан с атрибутом, который есть у каждого файла, — **Архивный (Archive).** Атрибут архивирования — это флаг, который устанавливается при создании или изменении файла. Для уменьшения размера и продолжительности заданий резервного копирования большинство типов архивации записывают на носитель только те файлы, у которых установлен атрибут архивирования. Чаще всего недоразумения возникают из-за терминологии. Например, фраза «Файл помечен как заархивированный», на самом деле означает, что атрибут архивирования сброшен после очередного задания архивации. Следующее задание архивации не будет копировать этот файл на носитель. Однако, если этот файл изменится, атрибут архивирования снова будет установлен, и файл запишется на носитель при следующем резервном копировании.

Обычная архивация

Архивируются все выбранные файлы и папки. Атрибут **Архивный (Archive)** сбрасывается. Обычная архивация не учитывает атрибут архивирования при определении файлов, подлежащих резервному копированию; все выбранные ресурсы записываются на целевой носитель. Каждая стратегия начинается с обычной архивации, которая по существу создает базовую линию, копируя все файлы в задании архивации.

По сравнению с другими типами обычная архивация выполняется дольше и требует больше места на носителе. Но, поскольку создается полная резервная копия данных, обычная архивация обеспечивает самую высокую скорость восстановления системы. Вам не придется восстанавливать несколько заданий. Обычная архивация сбрасывает атрибут архивирования у всех выбранных файлов.

Добавочная архивация

На целевой носитель копируются только выбранные файлы с установленным атрибутом архивирования, и флаг сбрасывается. Если

добавочная архивация выполняется на следующий день после обычной или другой добавочной архивации, копируются только созданные или измененные за последний день файлы.

Добавочная архивация самая быстрая и формирует архив минимального размера. Тем не менее, она не так эффективна, как обычная, поскольку требует восстановления сначала обычного архива, а затем всех последующих добавочных архивов в порядке их создания.

Разностная архивация

Копируются только выбранные файлы с атрибутом архивирования, и флаг не сбрасывается. Поскольку разностная архивация учитывает атрибут архивирования, копируются только файлы, созданные или измененные с момента последней обычной или добавочной архивации. Атрибут архивирования не сбрасывается, поэтому разностные архивы содержат не только созданные или измененные файлы, но и все файлы, скопированные при предыдущей разностной архивации. В результате резервные копии становятся больше, а сама разностная архивация длится дольше, чем добавочная, но меньше, чем обычная.

Разностная архивация, однако, значительно эффективнее добавочной в плане восстановления: требуется восстановить только обычный и последний разностный архивы.

Копирующая архивация

Архивируются все выбранные файлы и папки. Атрибут архивирования не учитывается. Копирующая архивация не применяется для обычного или планового резервного копирования. Ее удобно использовать для перемещения данных между системами или создания архивной копии данных на некоторый момент времени без вмешательства в стандартные процедуры резервного копирования.

Ежедневная архивация

Копируются все выбранные файлы и папки, измененные в течение дня с момента последней ежедневной архивации (на основе даты изменения файла). Атрибут архивирования не используется и не сбрасывается. Если вам нужно создать резервную копию файлов и папок, измененных за день, не составляя расписание, используйте ежедневную архивацию.

Совмещение типов резервного копирования

Хотя создание обычного архива каждую ночь обеспечивает возможность восстановления данных на следующий день с помощью одного задания, обычная архивация требует слишком много времени, и ночное задание может продлиться до утра, снижая производительность в рабочие часы. Чтобы выбрать оптимальную стратегию резервного копирования, необходимо учесть продолжительность и размер задания архивации, а также скорость восстановления системы в случае сбоя. Есть два типичных решения.

- **Обычная и разностная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — разностная. Разностная архивация не сбрасывает атрибут архивирования, поэтому каждая операция копирует все изменения, произошедшие с понедельника. В

случае сбоя данных в пятницу придется восстановить только обычный архив от воскресенья, и разностный от четверга. Такая стратегия требует больше времени для резервного копирования, особенно если данные изменяются часто, но восстановление происходит быстрее и удобнее, поскольку набор архивации занимает меньше дисков или лент.

- **Обычная и добавочная архивация.** В воскресенье выполняется обычная архивация, а с понедельника по пятницу — добавочная. Последняя сбрасывает атрибут архивирования, поэтому каждая операция архивации включает только файлы, изменившиеся со времени последнего резервного копирования. В случае сбоя данных в пятницу придется восстановить обычный архив, сделанный в воскресенье, и все добавочные архивы с понедельника по пятницу. Такая стратегия требует меньше времени на резервное копирование, но больше на восстановление.

Список использованной литературы

1. Расторгуев, Сергей Павлович. Основы информационной безопасности : [учеб. пособие*], 2-е изд., стер. - М. : Академия, 2009. - 188 с. - (Высшее проф. образование). - На обл.: Информационная безопасность. - Библиогр.: с. 180- 181. - ISBN 978-5-7695-6486-4.
2. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Изд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2006. - 208 с. - ISBN 5-9556-0052-3. - URL: http://biblioclub.ru/index.php?page=book&id=233063
3. Сычев, Ю.Н. Основы информационной безопасности : учебно-практическое пособие [Электронный ресурс] / Ю.Н. Сычев. - М. : Евразийский открытый институт, 2010. - 328 с. - ISBN 978-5-374-00381-9. - URL: http://biblioclub.ru/index.php?page=book&id=90790