Администрирование в информационных системах

Лекция 2.

Управление пользователями

Групповое управление безопасностью

Учетная запись

- Для управления пользователями в операционных системах используется понятие **учетной записи**.
- Учетная запись в доменах Microsoft используется специальный объект Active Directory, содержащий все атрибуты, позволяющие определить пользователя домена.
- К числу таких атрибутам относятся:
  - имя пользователя;
  - имена групп, членом которых является его учетная запись;
  - дополнительные атрибуты (имя, фамилия, телефоны и т.д.);
  - пароль.
- Учетные записи пользователей Windows хранятся либо в Active Directory (доменные записи), либо на локальном компьютере (локальные записи).
  - На компьютерах с Windows XP Professional и рядовых серверах с Windows Server 2003 управление локальными учетными записями пользователей осуществляется с помощью компонента «**Локальные пользователи и группы**».
  - На контроллерах домена под управлением Windows Server 2003 для этого используется компонент «**Active Directory — пользователи и компьютеры**».

Идентификатор безопасности

- Учетные записи пользователей и компьютеров (а также группы) называются **участниками безопасности**.
  - Участники безопасности являются объектами каталогов, которые автоматически назначают коды безопасности (SID) для доступа к ресурсам домена.
- **Идентификатор безопасности –** структура данных переменной длины, определяющая учетные записи пользователей, групп и компьютеров.
  - Идентификатор безопасности присваивается учетной записи при ее создании и не меняется при изменении атрибутов.
  - Внутренние процессы Windows обращаются к учетным записям по их SID, а не по именам пользователей или групп.

Использование учетных записей

- Учетная запись пользователя или компьютера используется для решения следующих задач:
  - **Проверка подлинности** пользователя или компьютера. Учетная запись пользователя дает право войти в компьютеры и в домен с подлинностью, проверяемой доменом. Для обеспечения максимальной безопасности не рекомендуется пользователям использовать одну и ту же учетную запись.
  - **Разрешение или запрещение доступа к ресурсам домена**. Как только проверка подлинности пользователя завершена, он получает или не получает доступ к ресурсам домена в соответствии с явными разрешениями, назначенными данному пользователю на ресурсе.
  - **Администрирование других участников безопасности**. Active Directory создает объект «**Участник внешней безопасности**» в локальном домене для представления каждого участника безопасности из внешнего доверенного домена.
  - **Аудит действий**, выполняемых с использованием учетной записи пользователя или компьютера.

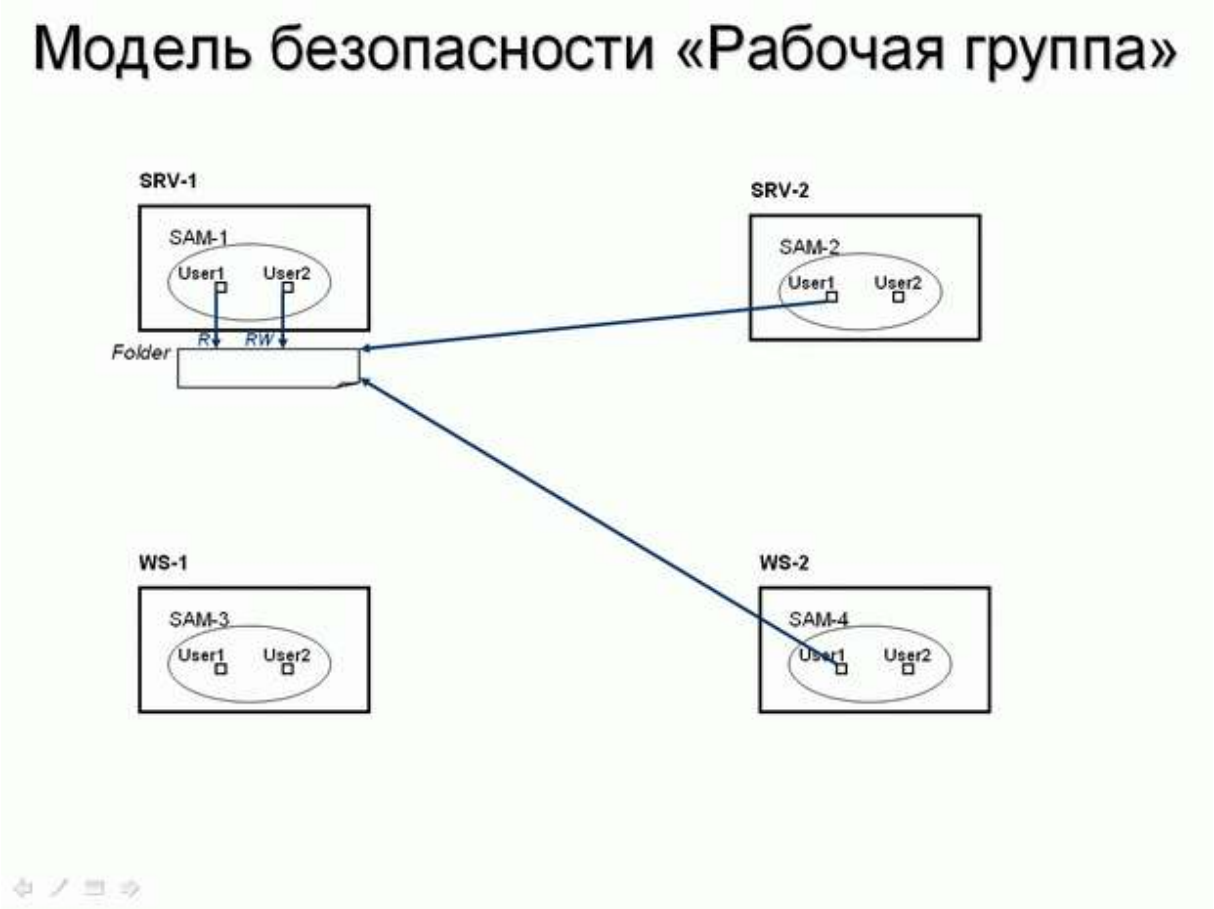
Управление пользователями

- Управление пользователями включает следующие функции администрирования:
  - Создание учетной записи для пользователя;
  - Изменение пароля;
  - Определение прав и разрешений для пользователя;
  - Отключение/включение учетной записи;
  - Удаление учетной записи пользователя.

Модель безопасности Рабочая группа

- Модель управления безопасностью корпоративной сети на основе Рабочей группы — самая примитивная.
  - Она предназначена для использования в небольших одноранговых сетях (3–10 компьютеров) и основана на том, что каждый компьютер в сети с операционными системами Windows NT/2000/XP/2003 имеет свою собственную локальную базу данных учетных записей и с помощью этой локальной БД осуществляется управление доступом к ресурсам данного компьютера.
- Локальная БД учетных записей называется база данных SAM (Security Account Manager) и хранится в реестре операционной системы. Базы данных отдельных компьютеров полностью изолированы друг от друга и никак не связаны между собой.

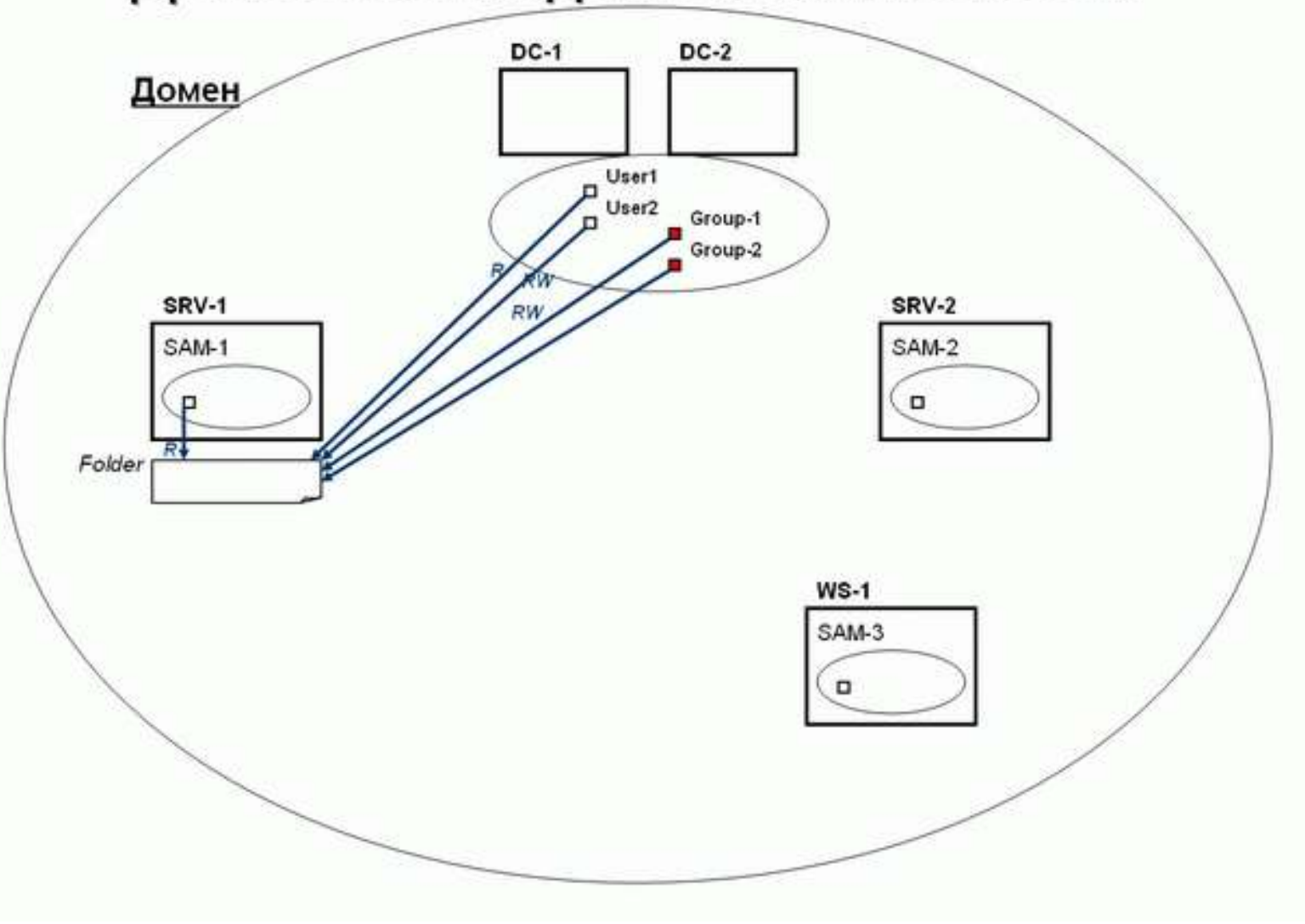
Управление безопасностью в модели Рабочая группа



Доменная модель безопасности

- В доменной модели существует единая база данных служб каталогов, доступная всем компьютерам сети.
- Для этого в сети устанавливаются специализированные серверы, называемые **контроллерами домена**, которые хранят на своих жестких дисках эту базу.

Доменная модель безопасности



Службы каталогов

- Основная цель объединения компьютеров в вычислительную сеть – обеспечение совместного использования ресурсов.
- Одна из основных решаемых задач – реализация оптимального метода организации общих ресурсов.
- В крупной организации речь идет о множестве ресурсов и множестве потребителей данных ресурсов.
- Для эффективного управления такими ресурсами применяются разные методы. Один из методов – развертывание *службы каталогов*.
- **Служба каталогов** – сетевая служба позволяющая пользователям получить доступ к ресурсу без знания точного месторасположения ресурса на основе именования в каталоге.
- При использовании службы каталогов вся информация об объектах сети объединяется в **каталог** (directory).
- Внутри каталога объекты организуются в соответствии с физической или логической структурой сети.

Службы каталогов

- Службы каталогов решают следующие задачи:
  - **Управление сетевыми ресурсами**. Служба каталогов облегчает пользователям поиск необходимых ресурсов, скрывая подробности реализации механизма поиска.
  - **Управление пользователями**. Каждый пользователь в сети идентифицируется набором реквизитов. Это позволяет осуществлять управление доступом к сетевым ресурсам.
  - **Управление приложениями**. В крупных вычислительных сетях возникает задача централизованного управления программным обеспечением, включая развертывание новых приложений и обновление существующих.
  - **Обеспечение функционирования сети**. Использование службы каталогов позволяет решить вопросы выделения IP-адресов, других параметров сети.
- **Сети Microsoft организуются с использованием службы каталогов Active Directory.**

Пространство имен X.500 и протокол LDAP

- Пространство имен (в соответствии со стандартом X.500) представляет собой иерархическую структуру имен, которая идентифицирует уникальный путь к контейнеру службы каталога.
- Это пространство имен определяется в числовой (точечной) нотации или в строковой.
- В строковой нотации пользовательский объект представляемый как:
  - cn=Dmitry, cn=Users, dc=Rosnou, dc=ru
  - Для удовлетворения требованию уникальности в пространстве имен X.500 в домене Rosnou.ru в контейнере Users может быть единственное имя Dmitry.

Протокол LDAP

- Протокол LDAP (облегченный протокол службы каталогов) является протоколом доступа. В данном протоколе для именования объектов используется система *характерных (различающихся) имен (Distinguish Name)*, предоставляющая информацию обо всех узлах дерева каталогов.
- Представление иерархии имен LDAP имеет вид:
  - LDAP: // cn=Dmitry, ou=faculty, dc=Rosnou, dc=ru
  - При записи характерного имени используются специальные ключевые слова:
    - DC – составная часть доменного имени;
    - OU – организационная единица;
    - CN – общее имя.
  - Имя, идентифицирующее сам объект, согласно терминологии LDAP, выступает в качестве относительного характерного имени. Относительное имя может быть не уникальным в рамках всего дерево, но должно быть уникальным в пределах контейнера.
  - *Каноническое имя* подобно характерному имени, за исключением того, что опускаются сокращения, обозначающие тип контейнера:
    - Rosnou.ru/faculty/Dmitry

Использование имен объектов системы

- Другой способ именования объектов – использование *основных имен* субъектов системы безопасности.
- Основное имя субъекта системы безопасности имеет вид:
  - <имя субъекта>@<суффикс основного имени>
  - В качестве суффикса основного имени выступает имя домена, которому принадлежит данный субъект
  - Пример основного имени пользователя:
    - dmitry@rosnou.ru
- Глобальные идентификаторы. Для обеспечения уникальности объектов и облегчения поиска, каждому объекту ставится в соответствие 128-разрядное число – *глобальный уникальный идентификатор*.
- Данный идентификатор является обязательным атрибутом любого объекта, который не изменяется ни при каких обстоятельствах.

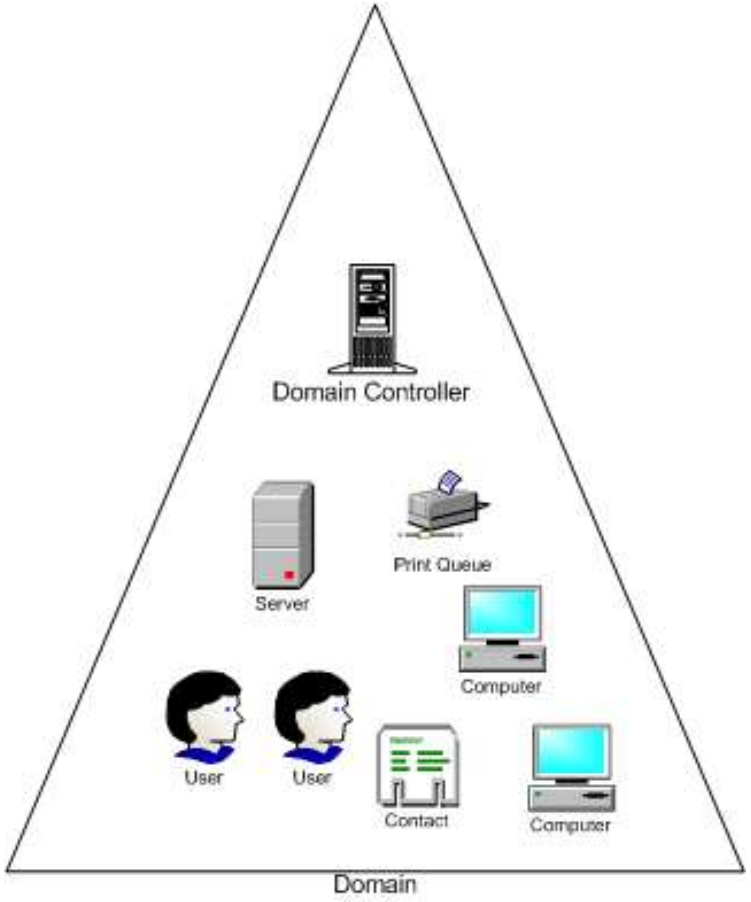
Доменная модель службы каталогов

- В рамках каталога Active Directory одним из основных понятий является понятие **домена** – *совокупность компьютеров, характеризующихся наличием общей базы учетных записей пользователей и единой политики безопасности*.

- Использование доменов позволяет разделить пространство имен на несколько фрагментов. Каждый объект может принадлежать **только** одному домену.
- Цели создания доменов:
  - **Разграничение административных полномочий.**
  - **Создание единой политики безопасности.**
  - **Разделение доменного контекста имен.**
- Центральным компонентом домена выступают серверы, хранящие фрагменты каталогов. Такие серверы называются **контроллерами домена**.

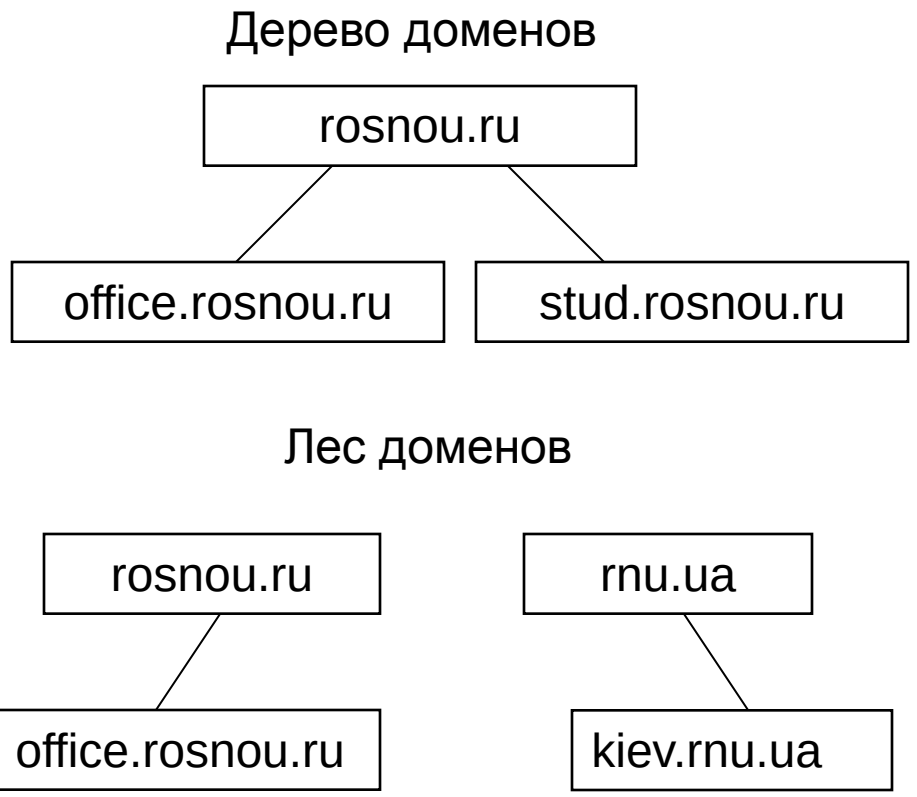
Домены Windows

- Домены Windows – группа компьютеров, связанных через вычислительную сеть, имеющая общую базу данных пользователей, общую политику безопасности, общее пространство имен, общие средства аутентификации и обеспечения безопасности.



Иерархия доменных имен

- Windows позволяет организовать разные типа иерархии доменов.
  - Отношение между доменами по схеме «родитель-потомок». Имя дочернего домена включает в себя имя родительского домена.
  - Отношения, включающие несколько связанных деревьев – лес доменов (forest).



Доверительные отношения

- Для объединения объектов, хранящихся в разных доменов должны существовать определенные связи – *доверительные отношения*.
- Механизм установленных доверительных отношений позволяет организовать процесс аутентификации объектов и субъектов системы.
- Выделяют два типа доверительных отношений:
  - **Односторонние доверительные отношения**
  - **Двусторонние доверительные отношения**

Контроллеры домена

- Контроллеры домена в доменах Windows отвечают за аутентификацию пользователей и содержат фрагмент каталога.
- Некоторые операции могут выполняться только одним контроллером. Эти операции называются *операции с одним исполнителем (flexible single-master operations – FSMO)*.
- Контроллеры доменов могут выполнять специализированные роли:
  - **Роли, требующие уникальности в пределах всего леса доменов:**
    - **Исполнитель роли владельца доменных имен**
    - **Исполнитель роли владельца схемы**
  - **Роли, требующие уникальности в пределах домена:**
    - **Исполнитель роли владельца идентификаторов**
    - **Исполнитель роли эмулятора основного контроллера домена**
    - **Исполнитель роли владельца инфраструктуры каталога.**
- По умолчанию все данные роли возлагаются на первый контроллер домена, установленный в лесе.
- Процесс принудительной передачи функций специализированной роли другому контроллеру называется *захватом роли*.

Разделы каталога

- В рамках каталога Active Directory выделяется несколько крупных фрагментов каталога – *разделов каталога*, представляющих законченные непрерывные поддеревья (контексты имен):
  - **Доменный раздел каталога**
  - **Раздел схемы каталога**
  - **Раздел конфигурации**
  - **Разделы приложений**
  - **Раздел глобального каталога**

Схема каталога

- Любой объект каталога принадлежит к некоторому классу объектов со своей структурой атрибутов.
- Определения всех классов объектов и совокупности правил, позволяющих управлять структурой каталога, хранится в специальной иерархической структуре – *схеме каталога*.
- Все данные схемы хранятся в виде двух классов объектов:
  - *Class Schema* – класс, определяющий типы объектов
  - *Attribute Schema* – класс, определяющий атрибут объекта. Каждый атрибут определяется в схеме один раз и может использоваться при описании множества классов объектов.
- Схема каталога хранится в отдельном разделе и допускает возможность расширения.

Раздел глобального каталога

- *Глобальный каталог* – специализированная база данных, содержащая фрагменты всех доменных контекстов имен.
- Для исключения чрезмерного разрастания базы данных в нее включены значения только наиболее часто используемых атрибутов.
- Контроллер домена, выступающий в качестве носителя такой базы данных, называется *сервером глобального каталога*. Он выполняется следующие функции:
  - *Предоставление пользователям возможности поиска объектов в лесу доменов по атрибутам*
  - *Разрешение основного имени пользователя*
  - *Предоставление информации о членстве пользователя в различных группах с универсальной областью действия.*
- В лесу доменов присутствует по крайней мере один сервер глобального каталога. По умолчанию это первый контроллер созданный в домене.

Другие разделы

- **Раздел конфигурации** – используется для размещения сведений о структуре системы: список всех доменов и деревьев леса, перечень существующих контроллеров домена и серверов глобального каталога.
- **Доменный раздел** – используется для размещения объектов, являющихся непосредственно частью домена. Здесь хранятся объекты, ассоциированные с пользователями, компьютерами, общими ресурсами. Данный раздел передается в рамках домена.
- **Разделы приложений** – могут быть созданы для различных сетевых приложений. Разделы могут быть созданы администратором вручную или самими приложениями при помощи интерфейса программирования ADSI (Active Directory Service Interfaces). Создание таких разделов позволяет обращаться к приложениям используя общий подход доменных имен.

Организационные единицы

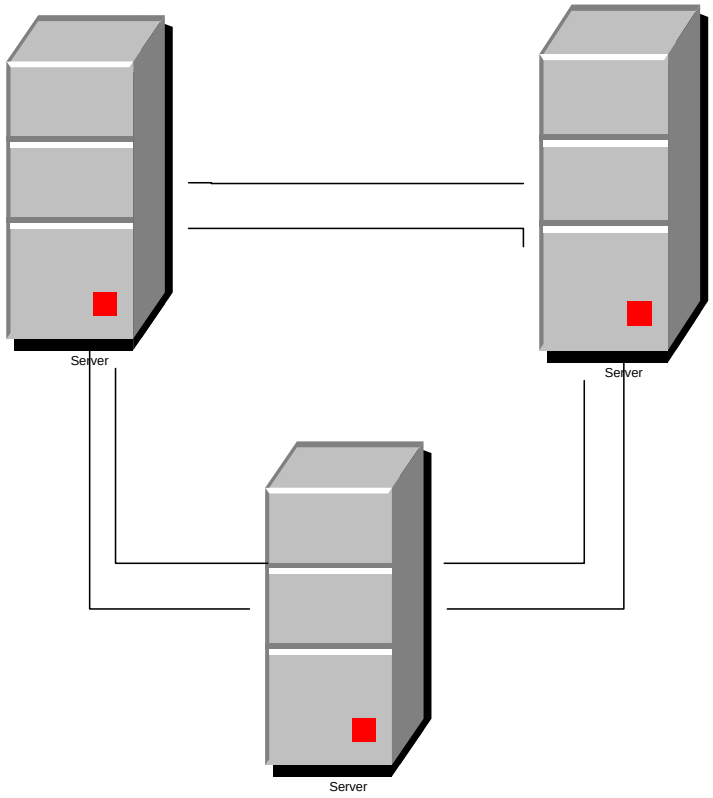
- В структуре службы каталога можно использовать специальные объекты контейнерного типа, позволяющие группировать объекты.
- Такими объектами являются *организационные единицы*, позволяющие объединять объекты в логическую структуру. Используются для упрощения управления входящими в них объектами.
  - Иерархия организационных единиц образуется только в пределах домена. Организационные единицы принадлежащие разным доменам леса не связаны друг с другом.

Физическая структура каталога. Репликация данных.

- **Корпоративная сеть** – *совокупность подсетей, соединенных между собой линиями связи*.
- Под узлом (site) в сетях Windows понимается совокупность подсетей объединенных высокоскоростными линиями связи.
- В структуре каталога существует специальный класс объектов, описывающий связи между узлами, - *соединение узлов*.
- Каждое соединение как объект каталога имеет следующие атрибуты:
  - Стоимость соединения
  - Расписание доступности соединения
  - Интервал репликации
  - Транспорт репликации
    - В качестве транспорта используются протоколы RPC и SMTP

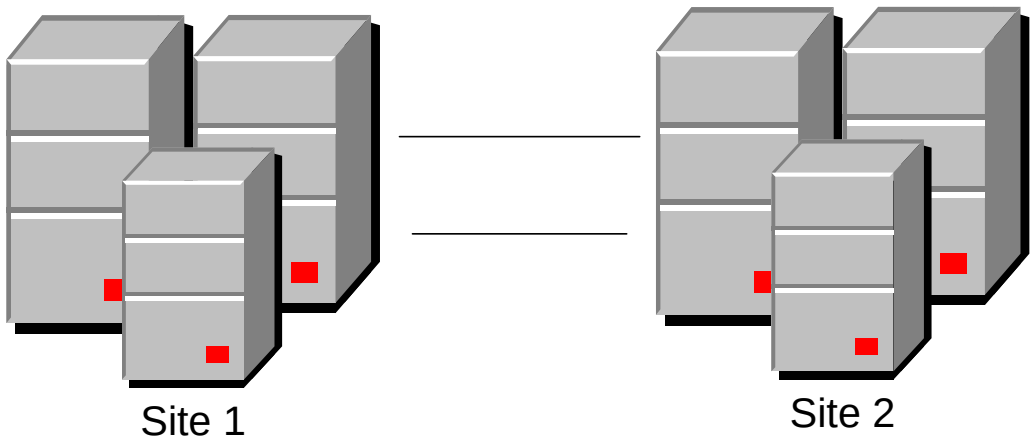
Репликация внутри узла

- При репликации баз данных каталога внутри узла осуществляется автоматически.
  - В процессе репликации используется кольцевая топология (двунаправленное кольцо).
- В процессе репликации применяется протокол RPC. Используется *синхронное взаимодействие* – принимающий партнер, отправляя запрос, ожидает ответа от передающего партнера.



Репликации между узлами

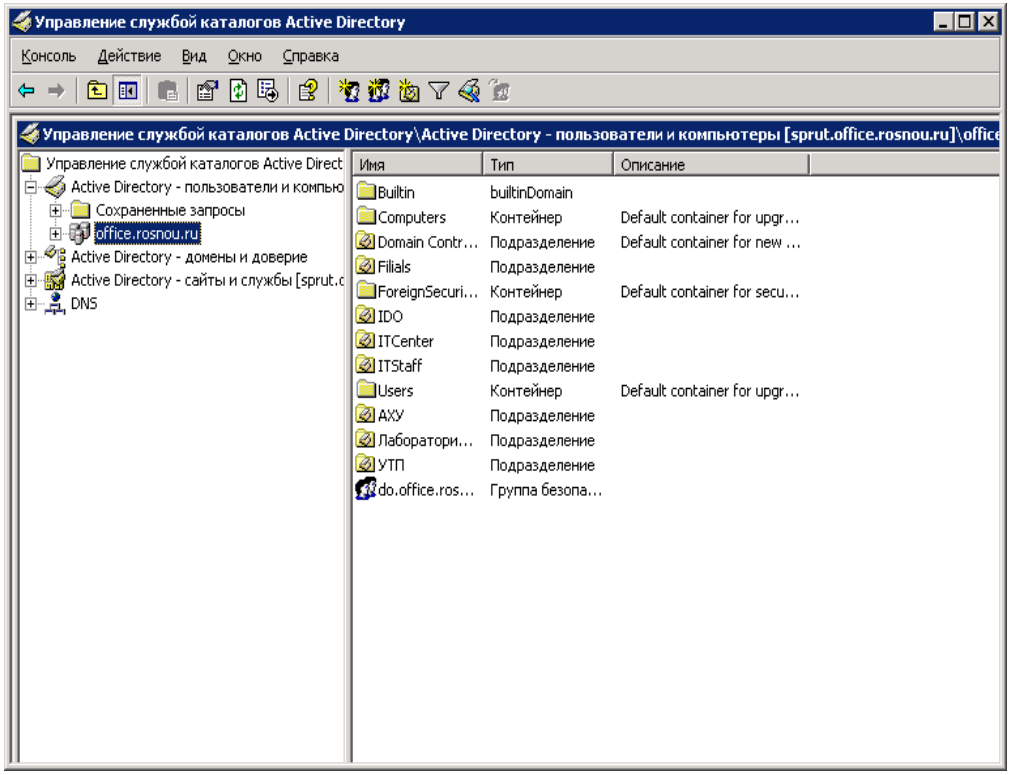
- Одной из причин объединения подсетей в узлы – необходимость управления процессом репликации между контроллерами домена на медленных линиях связи.
- В процессе репликации между узлами передается только информация об изменениях в схеме и данных конфигурации. Для серверов глобального каталога – данные о подмножестве объектов всех доменов, образующих лес.
- При передаче используются два протоколы: RPC и SMTP – для асинхронного взаимодействия.
- При репликации между узлами существенную роль играют *мостовые серверы*.



Управление службой Active Directory

- Для управления службой каталогов Active Directory используются специальные средства администрирования.

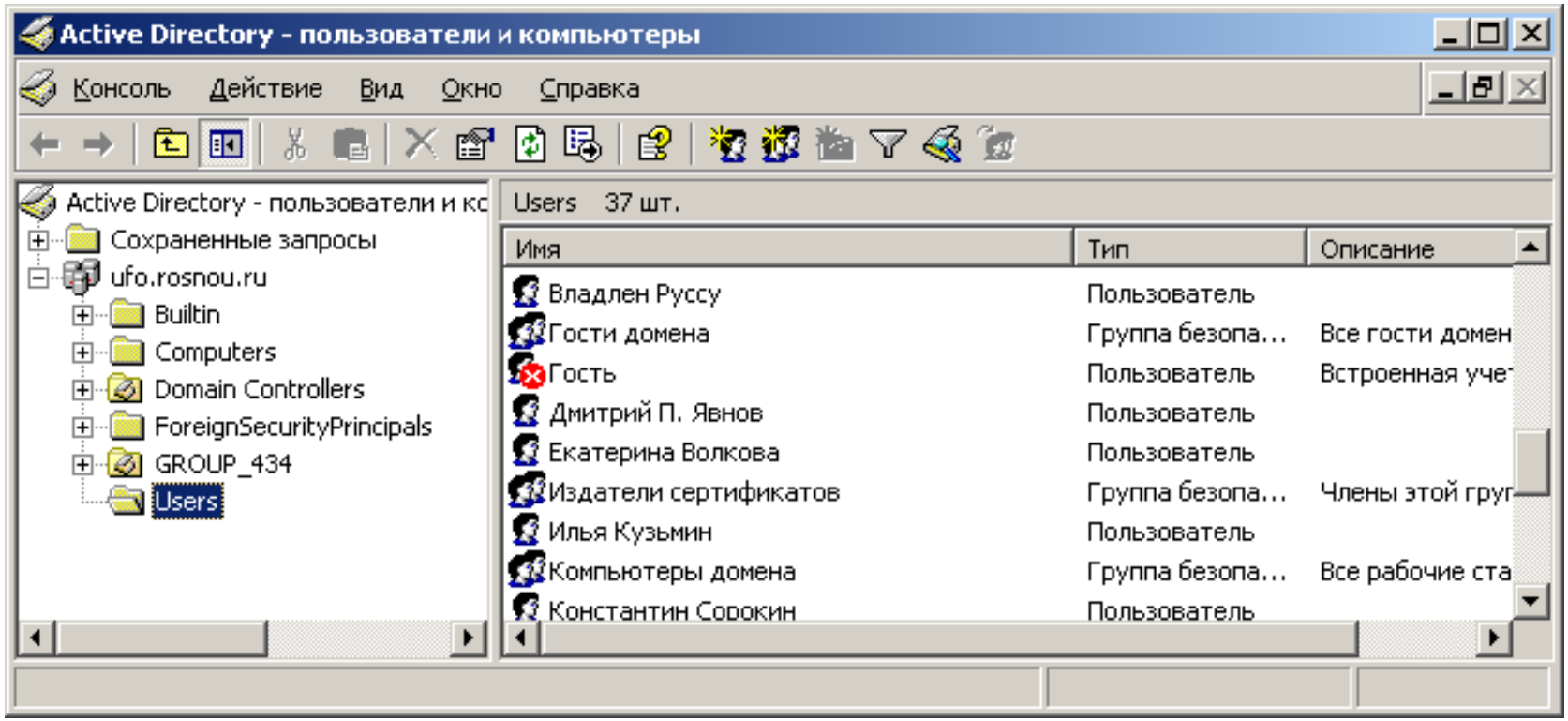
  - Утилиты администрирования службы каталогов:
    - Active Directory – пользователи и компьютеры
    - Active Directory – домены и доверие
    - Active Directory – сайты и службы



Инструменты управления учетными пользователями

- Для управления учетными записями пользователями в домене Windows 2003 можно использовать оснастку:
  - графические утилиты – оснастку Microsoft management console – **Active Directory — пользователи и компьютеры**;
  - утилиты командной строки – **dsadd user** и **net user**;
  - программный интерфейс – использование системных функций в программных модулях и сценариях (Visual Basic, C# и др.).

Графический интерфейс управления пользователями



Командный интерфейс управления пользователями

- Добавление пользователя в домен Windows осуществляется командой
  - **dsadd user**
- Пример использования:
  - **dsadd user "CN=Иван Петров, CN=Users, DC=UFO, DC=ROSNOU, DC=RU"**
  - Опциями команды являются:
    - - pwd – устанавливает новый пароль пользователя;
    - - mail – устанавливает адрес электронной почты
    - - mustchpwd yes|no – определяет должен ли пользователь поменять пароль при следующем входе
    - - canchpwd yes|no – определяет может ли пользователь изменить пароль
    - - disabled yes|no – определяет может ли пользователь войти в домен

Командный интерфейс управления пользователями

- Другие команды управления пользователями через командную строку:
  - dsmod user – внесение изменений в учетную запись пользователя
  - dsrm – удаляет пользователя из Active Directory
  - dsmove – перемещает учетную запись
  - dsquery user – запрашивает в Active Directory список пользователей по заданным критериям поиска
  - dsget user – показывает атрибуты заданного объекта

Командный интерфейс управления пользователями

- Упрощенной альтернативой является использование команды **net user**.
- Команды, позволяющие удаленно управлять пользователями через сеть, являются:
  - net user /domain – вывод списка пользователей домена
  - net user <name> <pwd> /add /domain – добавление пользователя в домен
  - net user <name> <pwd> /domain – изменение пароля пользователя
  - net user <name> /delete /domain – удаление пользователя
- Команда net accounts – позволяет выполнить настройку свойств учетной записи (мин. длина пароля и т.д.)

Использование программного интерфейса

- Для управления учетными записями пользователей может быть использован и программный интерфейс.
- Например, создание пользователя myUser в подразделении class112 (вложенного в подразделение hr) домена tc.ronou.ru

- provider = “LDAP://"
  OU = "ou=class112, ou=hr,"
  domain = "dc=tc,dc=rosnou, dc=ru"
  oClass = "User"
  oUname = "CN=myuser"
  Set objDomain = GetObject(provider & OU & domain)
  Set objUser = objDomain.create(oClass, oUname)
  objUser.Put "sAMAccountName", oUname
  objUser.SetInfo

Управление группами

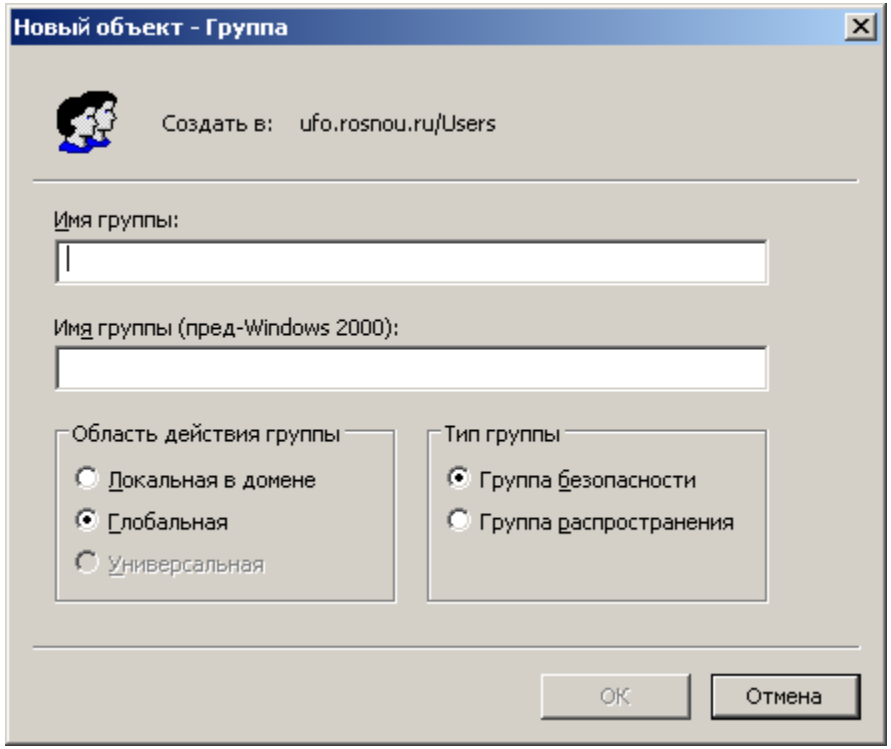
- Другая задача администрирования – управление группами.
- Управление группами включает в себя:
  - создание группы;
  - добавление пользователей в группу;
  - удаление группы.
- В Active Directory определены следующие типы групп безопасности:
  - локальные группы;
  - глобальные группы;
  - универсальные группы.

Группы безопасности

- **Локальная группа** – группа, права членства и доступа которой не распространяются на другие домены.
- **Глобальная группа** – определяет область действия как все деревья в лесе домена. Глобальная группа привязана к конкретному домену и в нее могут входить только объекты и другие группы, принадлежащие к данному домену.
- **Универсальная группа** – определяет область действия все домены в рамках того леса, в котором они определены. Универсальная группа может включать в себя объекты, ассоциированные с учетными записями пользователей, компьютеров и групп, принадлежащих любому домену леса.

Создание группа в Active Directory

- Графический интерфейса – использование оснастки **Active Directory — пользователи и компьютеры.**
  - **Группы распространения** применяются только в электронной почте.
  - **Группы безопасности** используются как для управления доступом, так и в качестве списков рассылки.



Командный интерфейс управления группами

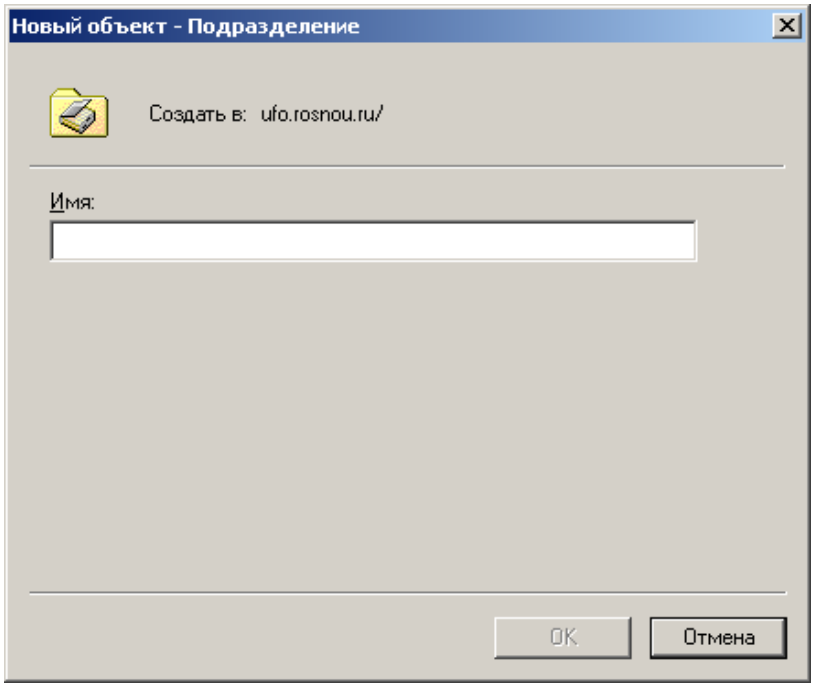
- Для управления группами можно использовать и команды управления объектами Active Directory:
  - dsadd group – добавляет группу
  - dsmod group – внесение изменений в учетную запись пользователя
  - dsrm – удаляет объект из Active Directory
  - dsquery group – запрашивает в Active Directory список групп по заданным критериям поиска
  - dsget group – показывает атрибуты заданного объекта

Управление группами в сетях Microsoft

- Другой вариант – применение команды **net group**:
  - net group <grp> /add /domain
  - net group <grp> /delete /domain
  - net localgroup <grp> /add /domain
  - net localgroup <grp> /delete /domain

Управление подразделениями

- Использование подразделений (организационных единиц – OU) представляет способ упрощения задач управления пользователями и компьютерами предприятия.
- Для создания нового подразделения необходимо воспользоваться командой контекстного меню оснастка **Active Directory — пользователи и компьютеры.**

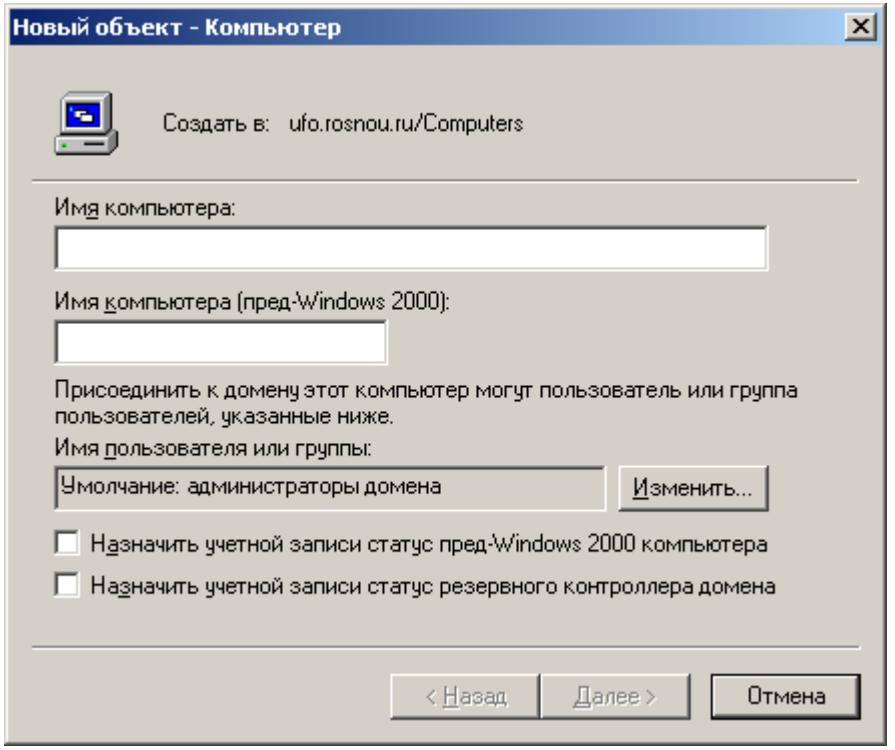


Управление организационными единицами

- Для управления подразделением, как объектом службы каталогов Active Directory используется команда **dsadd ou**
- Например для создания нового подразделения 434 в домене usfo.rosnou.ru:
  - dsadd ou “ou=434,dc=ufo,dc=rosnou, dc=ru”

Управление учетными записями компьютера

- Учетная запись, хранящаяся в Active Directory и однозначно определяющая компьютер в домене.
- Учетная запись компьютера соответствует имени компьютера в домене.
- Для добавления, изменения учетной записи компьютера можно использовать графический интерфейс оснастки **Active Directory — пользователи и компьютеры**



Управление учетными записями компьютеров

- Для управления учетными записями компьютеров можно воспользоваться утилитами командной строки **net computer** или dsadd computer.
- Например, команды:
  - net computer \\comp /add – добавление компьютера в домен
  - net computer \\comp /delete – удаление компьютера из домена
- Компьютеры имеют собственный идентификатор безопасности и могут участвовать в группах безопасности.

Безопасность в Active Directory

- Спецификации каталогов X.500 были определены в модели OSI в 1988 г.
  - Протокол службы каталогов является основным коммуникационным протоколом, использующимся для организации запросов к каталогу X.500.
- Lightweight Directory Access Protocol (LDAP) – основной протокол, используемый для доступа к Active Directory.
  - Для того, чтобы X.500-клиент мог организовать запрос к каталогу, необходимо установить сеанс связи с сервером каталога. Для установления связи необходимо пройти операцию **связывания,** требующую **аутентификации**.

Методы обеспечения безопасности

- **Аутентификация** – проверка подлинности пользователя, входящего в сеть Windows, с помощью Kerberos.
- **Доступ к объектам** – для управления доступом к объектам каталога используются списки контроля доступа (ACL).
- **Групповые политики** – Active Directory позволяет использовать политики, которые разрешают и запрещают доступ к ресурсам и участкам сети.

Схема Kerberos

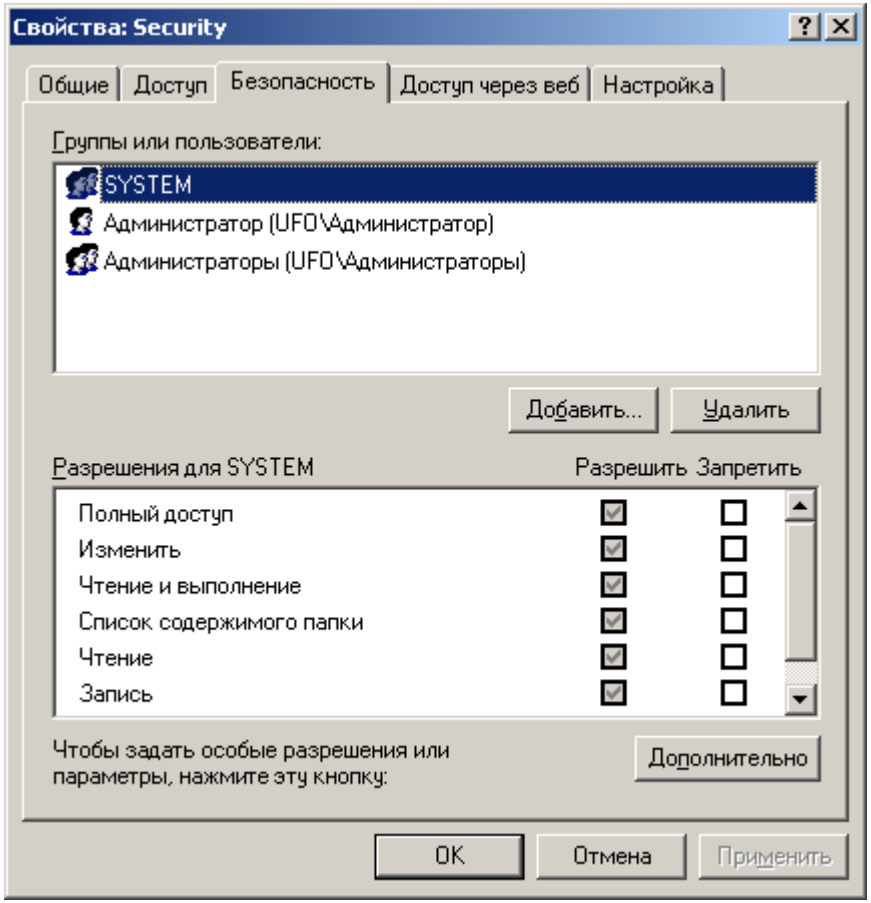
- Аутентификация Kerberos предназначена для решения задачи аутентификации субъектов в распределенной системе, использующей открытую сеть, с помощью **третьей доверенной стороны**.
- Система Kerberos , владеющая секретными ключами обслуживаемых субъектов, обеспечивает попарную проверку подлинности.
  - Для получения доступа к серверу S, клиент C отправляет на сервер Kerberos – K **запрос**, содержащий сведения о нем (клиенте) и о запрашиваемой услуге.
  - В ответ K возвращает **билет,** зашифрованный секретным ключом сервера и копию части информации из билета, зашифрованную секретным ключом клиента. C расшифровывает вторую порцию билета и пересылает ее вместе с билетом серверу S.
  - Сервер S расшифровав билет, сравнивает с дополнительной информацией, присланной клиентом. Совпадение свидетельствует, что клиент смог расшифровать предназначенные ему данные. Это и подтверждает подлинность клиента.

Списки контроля доступа

- Список средств защиты, которые применяются для всего объекта, набора его свойств или для его отдельного свойства.
- Существует два типа таблиц управления доступом:
  - **избирательные** (DACL) – часть дескриптора безопасности объекта, предоставляющая или запрещающая доступ к объекту для конкретных пользователей или групп. Изменять разрешения управления в избирательной таблице доступом может только владелец объекта;
  - **системные** (SACL) – часть дескриптора безопасности объекта, определяющая перечень проверяемых событий для пользователя или группы. Примерами таких событий являются: доступ к файлам, вход в систему, выключение системы .

Управление доступом

- Для управления доступом к объектам в Windows используется список контроля доступа, для получения данного списка используется закладка **Безопасность** в контекстном меню объекта
  - В качестве объектов могут выступать файлы, папки, разделы реестра Windows и другие объекты.
  - *Для файлов и папок необходимо, чтобы данный раздел был отформатирован в виде файловой системы NTFS.*



Групповые политики

- Инфраструктура в рамках службы каталогов Active Directory, обеспечивающая изменение и настройку параметров пользователей и компьютеров, включая безопасность и данные пользователя, на основе каталогов.
- Групповая политика используется для определения конфигураций для объединений учетных записей пользователей и компьютеров.
  - С помощью групповой политики можно задавать параметры политик на основе реестра, безопасности, установки программного обеспечения, сценариев, перенаправления папки, служб удаленного доступа и Internet Explorer.

Параметры групповой политики

- Параметры созданной пользователем групповой политики содержатся в объекте групповой политики (GPO).
  - Объект групповой политики может быть связан с контейнерами Active Directory:
  - сайтами,
  - доменами
  - подразделениями;
- В качестве объектов применения параметров политики выступают пользователи и компьютеры в соответствующих контейнерах Active Directory.
- Для создания GPO используется редактор объектов групповой политики. Для управления объектами групповой политики на предприятии можно использовать консоль управления групповой политикой (GPMC).