

# Администрирование информационных систем

Группы безопасности  
Управление  
пользователями

# Учетная запись

- Для управления пользователями в MS Windows используется понятие **учетной записи**.
- Учетная запись в Active Directory — объект, содержащий все сведения, позволяющие определить пользователя домена.
- К таким сведениям относятся:
  - имя пользователя,
  - пароль
  - группы, членом которых является его учетная запись.
- Учетные записи пользователей хранятся либо в Active Directory, либо на локальном компьютере.
  - 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**».

# Код 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.
- **Код безопасности** – структура данных переменной длины, определяющая учетные записи пользователей, групп и компьютеров. Код безопасности присваивается учетной записи при ее создании. Внутренние процессы Windows

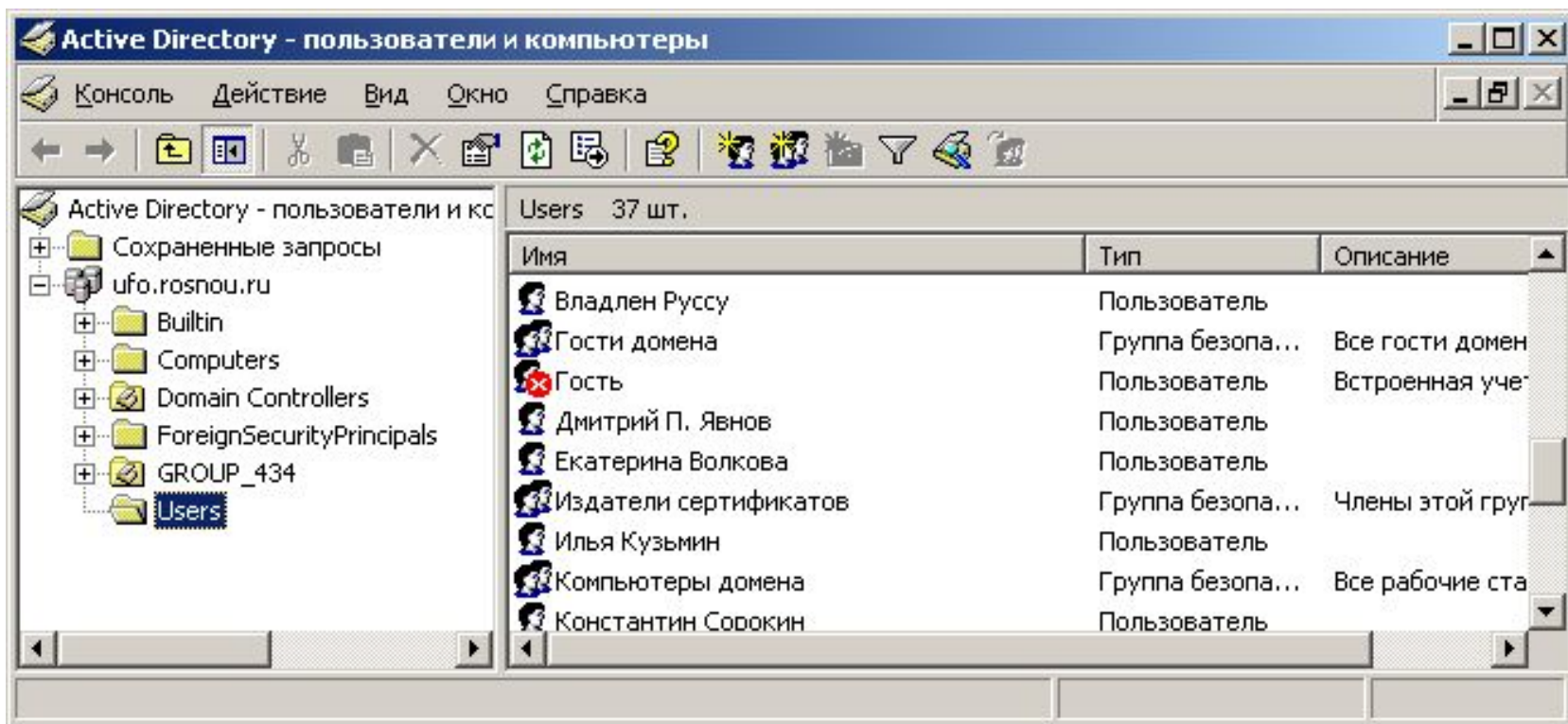
# Использование учетных записей

- Учетная запись пользователя или компьютера используется для следующих целей:
  - **Проверка подлинности** пользователя или компьютера. Учетная запись пользователя дает право войти в компьютеры и в домен с подлинностью, проверяемой доменом. Каждый входящий в сеть пользователь должен иметь собственную учетную запись и пароль. Для обеспечения максимальной безопасности следует запретить 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 такие функции:
  - Создание учетной записи для пользователя;
  - Изменение пароля;
  - Отключение/включение учетной записи;
  - Удаление учетной записи пользователя.
- Для управления учетными записями в домене Windows 2003 можно использовать оснастку **Active Directory** — **пользователи и компьютеры** или команду **dsadd user**.

# Графический интерфейс управления пользователями



# Командный интерфейс управления пользователями

- Добавление пользователя в домен Windows осуществляется командой
  - **dsadd user**
  - **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 user` – удаляет пользователя из Active Directory
  - `dsmove user` – 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

- 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
  - `net accounts` – настройка свойств учетной записи (мин. длина пароля и т.д.)

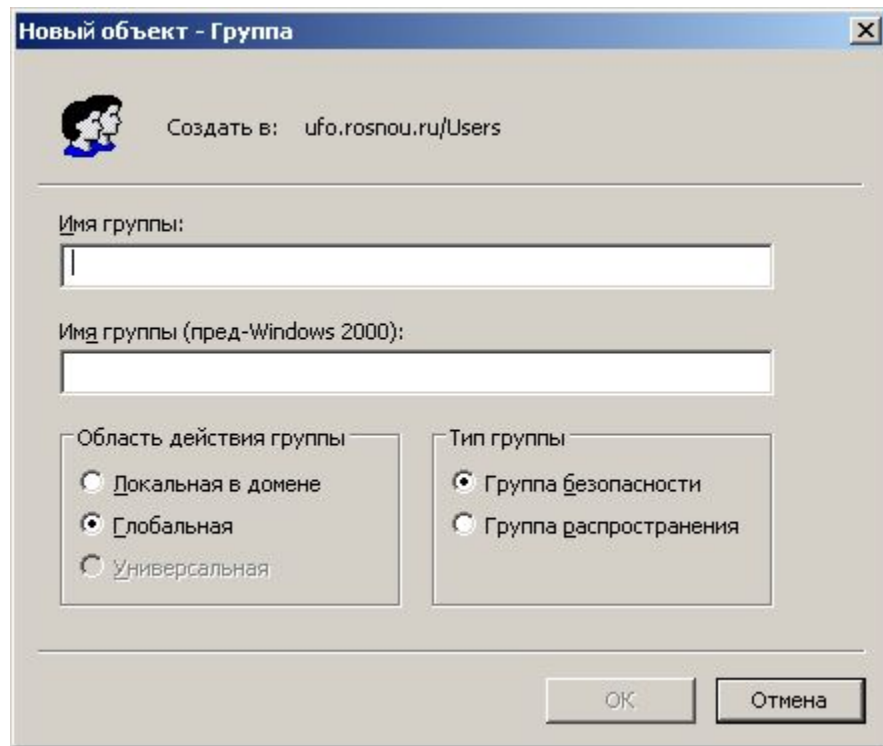
# Управление группами

- 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

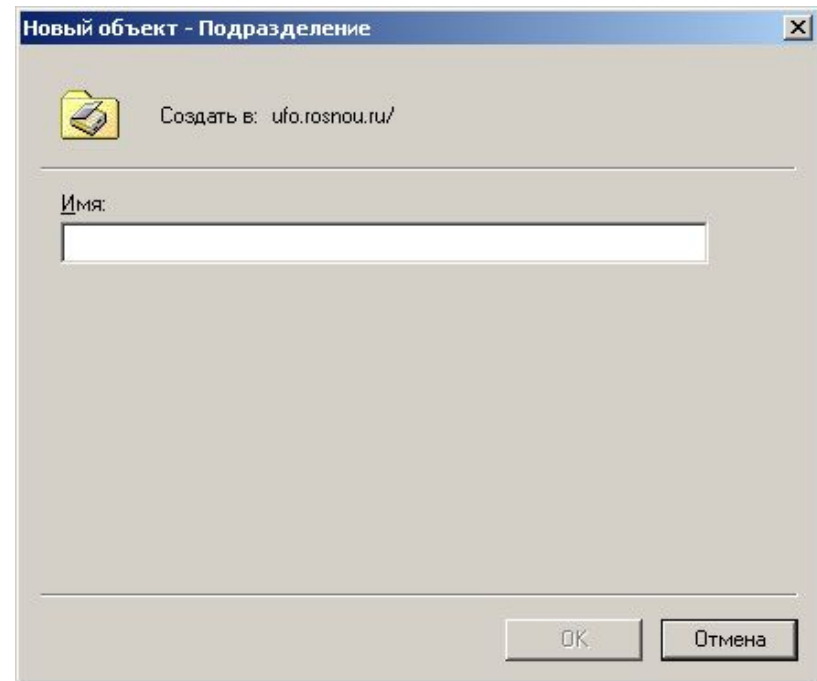


# Командный интерфейс управления группами

- 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
- Другой вариант – применение команды `net`:
  - `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.
- Управление подразделениями включает в себя задачи создания и удаления организационных единиц.
- Для создания нового подразделения необходимо воспользоваться командой контекстного меню оснастка **Active Directory — пользователи и компьютеры**.
- Для управления подразделением, как объектом службы каталогов Active Directory применяется условное обозначение OU, например:
  - `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, как графический интерфейс оснастки **Active Directory — пользователи и компьютеры**, так и командный интерфейс.
- Например, команды:
  - net computer [\\comp](#) /add
  - net computer [\\comp](#) /delete
- Компьютеры могут участвовать в группах безопасности.

Новый объект - Компьютер

Создать в: ufo.rosnou.ru/Computers

Имя компьютера:

Имя компьютера (пред-Windows 2000):

Присоединить к домену этот компьютер могут пользователь или группа пользователей, указанные ниже.

Имя пользователя или группы:

Умолчание: администраторы домена Изменить...

Назначить учетной записи статус пред-Windows 2000 компьютера

Назначить учетной записи статус резервного контроллера домена

< Назад Далее > Отмена

# Внесение пакетных изменений

- Команды службы каталогов полезны при работе с несколькими пользователями, компьютерами или подразделениями.
- Для повышения эффективности работы с сотнями объектов Active Directory можно использовать команды пакетных изменений:
  - `csvde` – Импорт и экспорт данных из Active Directory с помощью файлов, хранящих данные в формате CSV (comma-separated value). Кроме того, возможна поддержка пакетных операций на основе файлового стандарта CSV.
  - `ldifde` – Служебный инструмент, позволяющий производить пакетные изменения. Создает, изменяет и удаляет объекты папок на компьютерах с операционной системой Windows Server 2003 или Windows XP Professional. Пользователь может также использовать `Ldifde` для расширения схемы, экспорта сведений Active Directory о пользователе и группе в другие приложения или службы и для заполнения Active Directory данными из других служб каталогов.



# Безопасность в Active Directory

- Спецификации каталогов X.500 были определены в одеде OSI в 1988 г. Протокол службы каталогов является основным коммуникационным протоколом, используемым 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.**

# Защита Active Directory

- Для обеспечения безопасности хранимой информации в Active Directory необходимо решить вопросы:
  - Каким образом разрешается доступ для зарегистрированных пользователей?
  - Каким образом запрещается доступ к конфиденциальным данным для незарегистрированных пользователей?
  - Каким образом разделяется доступ к информационным объектам для различных пользователей?

# 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

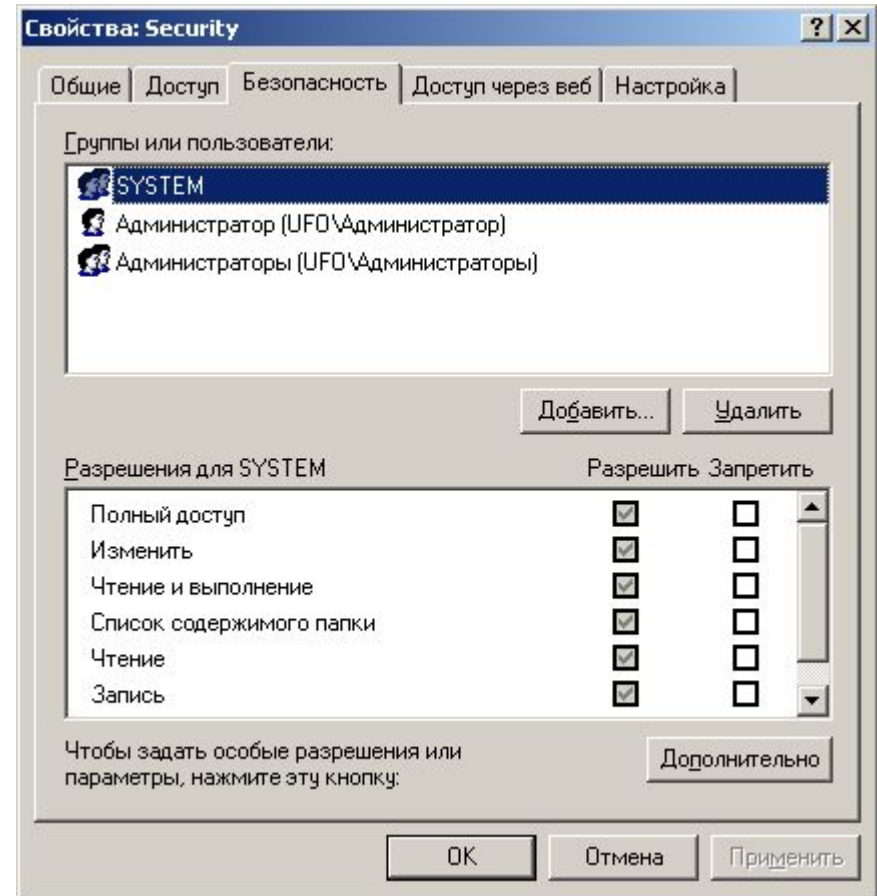
- Аутентификация Kerberos предназначена для решения задачи аутентификации субъектов в распределенной системе, использующей открытую сеть, с помощью **третьей доверенной стороны**.
- Система Kerberos, владеющая секретными ключами обслуживаемых субъектов, обеспечивает попарную проверку подлинности.
- Для 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
- Добавляя пользователей и задавая им разрешения в нижней части окна, определяются права доступа пользователя или группы к выбранному объекту.
- 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.



# Управление доступом

- Для управления доступом может быть использован и командный интерфейс:
- **cacls** *имя\_файла* [**/t**] [**/e** [**/r** *пользователь* [...]]] [**/c**] [**/g** *пользователь:разрешение*] [**/p** *пользователь:разрешение* [...]] [**/d** *пользователь* [...]]
- **Параметры:**
- *имя\_файла* Обязательный параметр. Вывод избирательных таблиц управления доступом (DACL) указанных файлов.
- **/t** Изменение избирательных таблиц контроля доступа (DACL) указанных файлов в текущем каталоге и всех подкаталогах.
- **/e** Редактирование избирательной таблицы управления доступом (DACL) вместо ее замены.
- **/r** *пользователь* Отмена прав доступа для указанного пользователя. Недопустим без параметра **/e**.
- **/c** Продолжение внесения изменений в избирательные таблицы управления доступом (DACL) с игнорированием ошибок.
- **/g** *пользователь:разрешение*
  - Предоставление прав доступа указанному пользователю. В следующей таблице перечислены допустимые значения параметра *Разрешение*.
    - **n** - Нет **r** - Чтение **w** - Запись **c** - Изменение (запись) **f** - Полный доступ
- **/p** *пользователь:разрешение* Смена прав доступа для указанного пользователя.
  - **n** - Нет **r** - Чтение **w** - Запись **c** - Изменение (запись) **f** - Полный доступ
- **/d** *пользователь*
  - Запрещение доступа для указанного пользователя.

# 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 групп 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 созданной пользователем групповой политики содержатся в объекте групповой политики (GPO). Связав GPO с выбранными контейнерами Active Directory; сайтами, доменами и подразделениями; можно применить параметры политики этого GPO к пользователям и компьютерам 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).



# Анализ и настройка безопасности

- Оснастка «Анализ и настройка безопасности» используется для анализа и настройки безопасности локального компьютера.

Средство управления настройкой безопасности	Описание
<a href="#">Шаблоны безопасности</a>	Определение политики безопасности в шаблоне. Эти шаблоны могут применяться к групповой политике или к локальному компьютеру.
<a href="#">Расширение «Параметры безопасности» для групповой политики</a>	Изменение отдельных параметров безопасности домена, узла или подразделения
<a href="#">Локальная политика безопасности</a>	Изменение отдельных параметров безопасности локального компьютера.
<a href="#">Secedit</a>	Автоматизация выполнения задач по настройке безопасности с помощью командной строки.

# Шаблоны безопасности

- **Шаблоны безопасности** (Security Templates) – файл, содержащий параметры безопасности. Шаблоны безопасности могут быть применены на локальном компьютере, импортированы в объект групповой политики или использованы для анализа безопасности.
- Для управления шаблонами используется изолированная оснастка mmc, позволяющая создавать текстовые файлы шаблонов, которые содержат параметры настройки безопасности.
- **Конфигурации безопасности** может быть применена к локальному компьютеру или импортирована в объект групповой политики (GPO) Active Directory.
- При импорте шаблона безопасности в GPO групповая политика обрабатывает шаблон и соответствующим образом изменяет члены GPO, которыми могут являться пользователи или компьютеры.

# Примеры шаблонов безопасности

- В Windows 2003 существует несколько готовых шаблонов безопасности:
  - Setup security и DC security – шаблоны по умолчанию для рядового сервера и контроллера домена
  - Compatws – используется, чтобы устранить необходимость вхождения пользователей в группу «Опытные пользователи»
  - Securews повышает безопасность путем удаления всех членов группы «Опытные пользователи» на компьютерах работающих под управлением Windows 2000 и XP.
  - Hisecws и HisecDC используется для работы в однородном домене Windows 2000, 2003.
- Готовые шаблоны безопасности представляют собой отправную точку в создании политик безопасности, которые настраиваются, чтобы удовлетворять организационным требованиям.
- По умолчанию готовые шаблоны безопасности сохранены в расположении:
  - *системный\_корневой\_каталог\Security\Templates*

# Стандартные шаблоны безопасности

- **Безопасность по умолчанию (Setup security.inf)**
- Шаблон Setup security.inf создается во время установки для каждого компьютера. Шаблон может различаться на разных компьютерах, в зависимости от того, производилась ли новая установка или обновление.
- Шаблон Setup security.inf содержит параметры безопасности, используемые по умолчанию, которые применяются во время установки операционной системы, включая разрешения для файлов корневого каталога системного диска. Он может быть использован на компьютерах-серверах и компьютерах-клиентах, но не на контроллерах домена. Части этого шаблона могут быть использованы для восстановления системы после сбоя.
- Шаблон Setup security.inf нельзя применять при помощи оснастки «Групповая политика». Данный шаблон имеет большой объем, при его применении с помощью оснастки «Групповая политика» возможно серьезное снижение производительности в связи с периодическим обновлением политики и перемещением значительного объема данных в домене.
- Шаблон рекомендуется применять по частям. Рекомендуется использование средства командной строки Secedit, дающего такую возможность.

# Стандартные шаблоны безопасности

- **Безопасность по умолчанию для контроллеров домена (DC security.inf)**
- Данный шаблон создается при назначении сервера контроллером домена. Он отражает настройки безопасности, используемые по умолчанию для файлов, реестра и системных служб.
- Применение этого шаблона приводит к установке значений по умолчанию в данных областях, но может перезаписать разрешения для новых файлов, ключей реестра и системных служб, созданных другими приложениями.
- Шаблон может быть применен с помощью оснастки «Анализ и настройка безопасности»

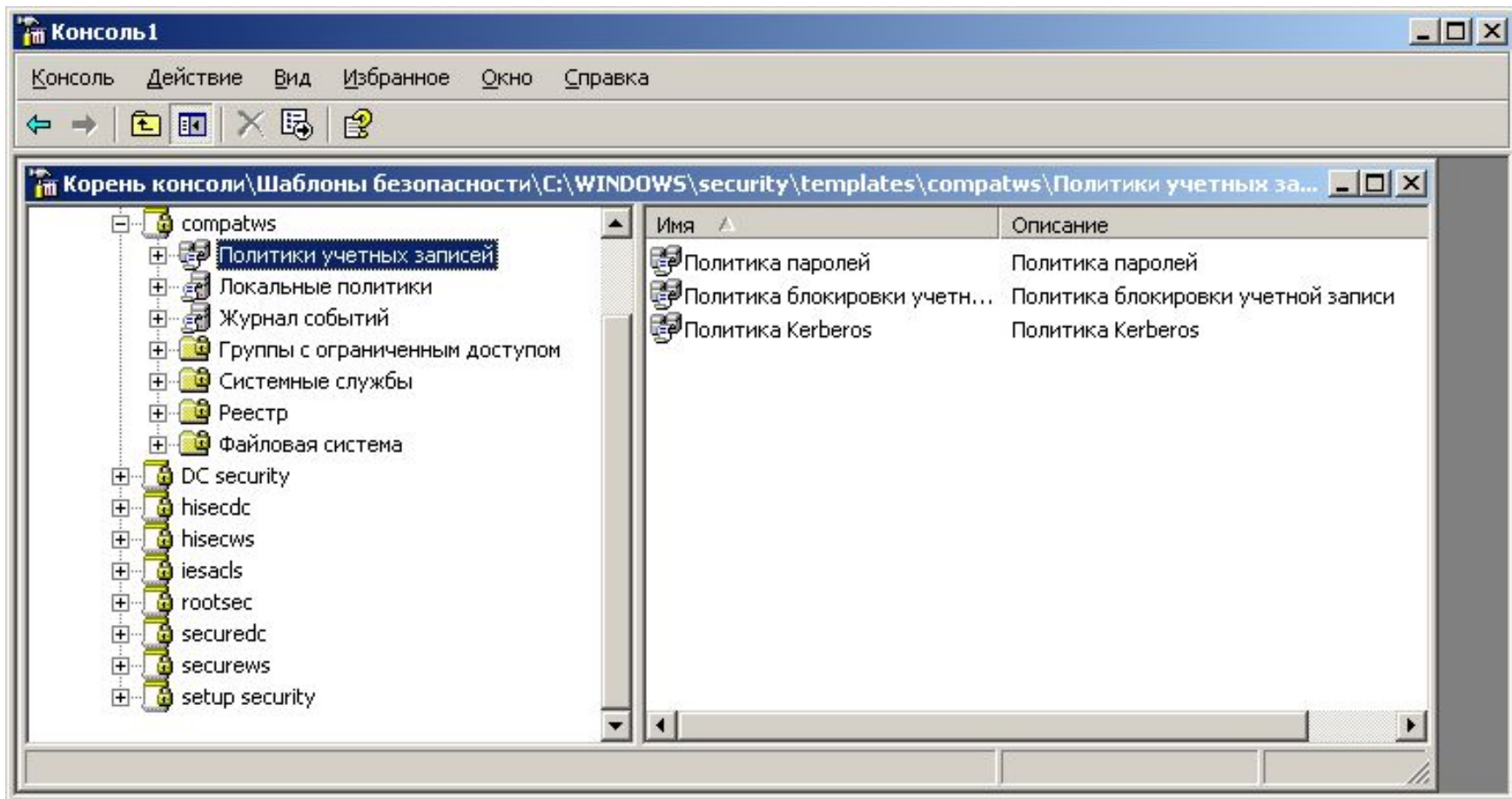
# Стандартные шаблоны безопасности

- **Совместимый (Compatws.inf)**
- Разрешения по умолчанию для рабочих станций и серверов сначала создаются для их локальных групп: «Администраторы», «Опытные пользователи» и «Пользователи». Члены группы «Администраторы» обладают наибольшими правами, тогда как члены группы «Пользователи» — наименьшими, можно значительно повысить безопасность, надежность и снизить общую стоимость владения системой, если придерживаться следующих правил:
  - убедиться, что конечные пользователи являются членами группы «Пользователи»;
  - внедрить приложения, которые могут успешно запускаться и выполняться членами группы «Пользователи».
- Лица, обладающие правами группы «Пользователи» могут работать с сертифицированными приложениями
- Члены группы «Опытные пользователи» обладают наследуемыми возможностями, такими как создание пользователей, групп, принтеров и общих ресурсов, некоторые администраторы предпочитают предоставить дополнительные разрешения группе «Пользователи», вместо зачисления конечных пользователей в группу «Опытные пользователи». Для этих целей служит «Совместимый» шаблон.
- При помощи шаблона «Совместимый» можно изменить разрешения для файлов и реестра, используемые по умолчанию для группы «Пользователи», и соответствующие требованиям большинства приложений, не входящих в число сертифицированных.

# Стандартные шаблоны безопасности

- **Защита (Secure\*.inf)**
- В шаблоне «Защита» определяются параметры повышенной безопасности. Наименее вероятно, что они оказывают влияние на совместимость. Например, в шаблоне «Защита» определяются параметры надежных паролей, блокировки и аудита.
- Помимо этого, шаблоном «Защита» ограничивается использование LAN Manager и протоколов проверки подлинности NTLM путем настройки клиентов на отправку ответов в формате NTLMv2, а также настройки серверов на отказ от ответов в этом формате.
- Шаблоны безопасности также определяют дополнительные ограничения для анонимных пользователей. Анонимные пользователи (такие как пользователи доменов, с которыми не установлены доверительные отношения) не могут выполнять следующие действия.
  - Ввод имен учетных записей и общих ресурсов.
  - Выполнение перевода [SID](#)-имя или имя-SID.
- Шаблоны безопасности включают подпись пакетов SMB на сервере, которая по умолчанию отключена для серверов. Поскольку подпись пакетов SMB на стороне клиента включена по

# Графический интерфейс работы с шаблонами безопасности





# Анализ и настройка безопасности

- Для тестирования шаблонов безопасности в Windows может быть использован графический интерфейс оснасти «**Анализ и настройка безопасности**».
- При выполнении прогнозов безопасности данный инструмент анализирует параметры настройки безопасности на локальном компьютере и сравнивает ее с тем шаблоном, что вы собираетесь применить. Данная операция производится путем импорта шаблона (.inf-файла) в файл базы данных(.sdb-файл).
- Командный интерфейс для выполнения анализа шаблонов задается командой:
  - secedit
    - secedit /analyze
    - secedit /configure
    - secedit /export
    - secedit /import
    - secedit /validate
    - secedit /GenerateRollback