

Лекция 7. Групповые политики доменов. Объекты групповых политик (GPO)

Групповые политики

- Структура многопользовательских операционных систем предполагает возможность создания для отдельного пользователя индивидуального окружения.
- В окружение пользователя могут входить:
 - конфигурации рабочего стола и индивидуальные настройки оболочки;
 - доступные пользователю приложения;
 - сценарии, выполняющиеся при входе пользователя в систему или выходе из нее;
 - ассоциированные с пользователем права и разрешения на доступ к локальным и сетевым информационным ресурсам.
- Для управления разрешениями пользователей в доменах Windows используется механизм **групповых политик**.

Понятие групповой политики домена

- Под **групповой политикой** понимается совокупность параметров, используемых для конфигурирования рабочего окружения пользователя или компьютера.
- Механизм групповых политик – основа централизованного управления конфигурациями пользователей и компьютеров в корпоративной сети.

Основные категории сетевых объектов домена

- Групповая политика в доменах Windows применяется к двум основным категориям сетевых объектов – **компьютерам и пользователям домена.**

Пользователи	Групповая политика регламентирует окружение конкретных пользователей независимо от того, на каком компьютере эти пользователи работают
Компьютеры	Групповая политика определяет параметры системы, влияющие на окружение пользователей, для конкретных компьютеров независимо от того, какие пользователи на них работают

Применение групповых политик

- Особенности групповых политик:
 - объекты GPO применяются в отношении контейнеров, а не замыкающих объектов;
 - один контейнер может быть связан с несколькими объектами GPO;
 - объекты GPO, связанные с одним и тем же контейнером, применяются в отношении этого контейнера в том порядке, в котором они были назначены;
 - объект GPO включает в себя две составляющие: параметры, относящиеся к компьютеру, и параметры, относящиеся к пользователю;
 - обработку любой из этих составляющих можно отключить;
 - наследование объектов GPO можно блокировать;
 - наследование объектов GPO можно форсировать;
 - применение объектов GPO можно фильтровать при помощи списков ACL

Объекты групповой политики

- **Объекты групповой политики (GPO)** – основной элемент групповой политики, выступающий в качестве самостоятельных элементов каталога.
 - Объекты групповой политики входят как объекты службы каталогов Active Directory.
- С каждым объектом групповой политики связан глобальный уникальный идентификатор – GUID.
- Для управления ими используются специальные инструменты – *редакторы групповых политик, программные интерфейсы.*

Локальная групповая политика

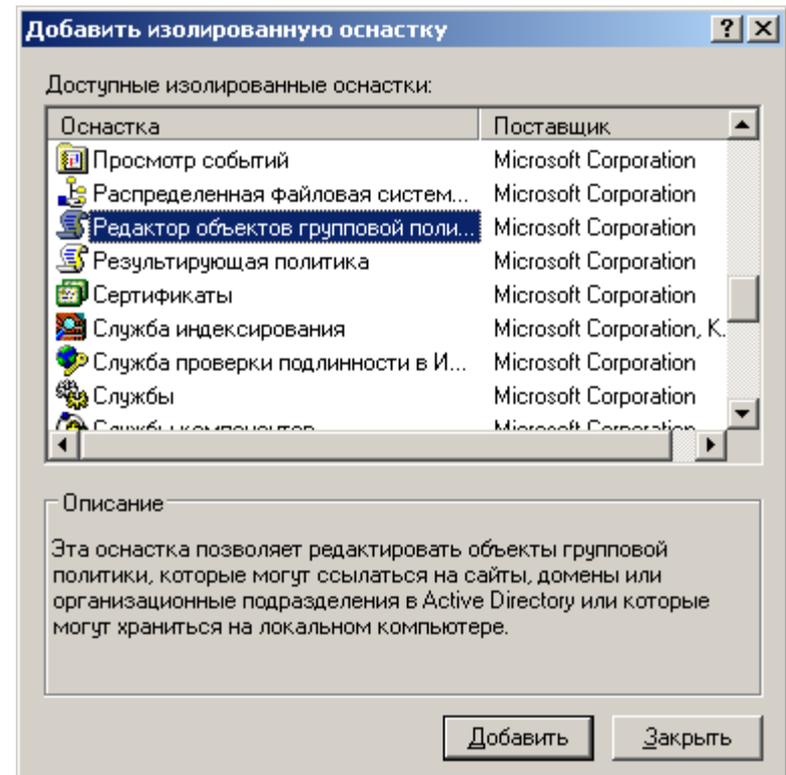
- Любой объект групповой политики может быть связан с некоторым объектом контейнерного типа в каталоге, относящемся к одному из трех классов:
 - Узел (сайт);
 - Домен;
 - Организационная единица.
- На каждом компьютере, под управлением Windows существует специальный объект групповой политики – **локальная групповая политика**.

Размещение объектов групповой политики

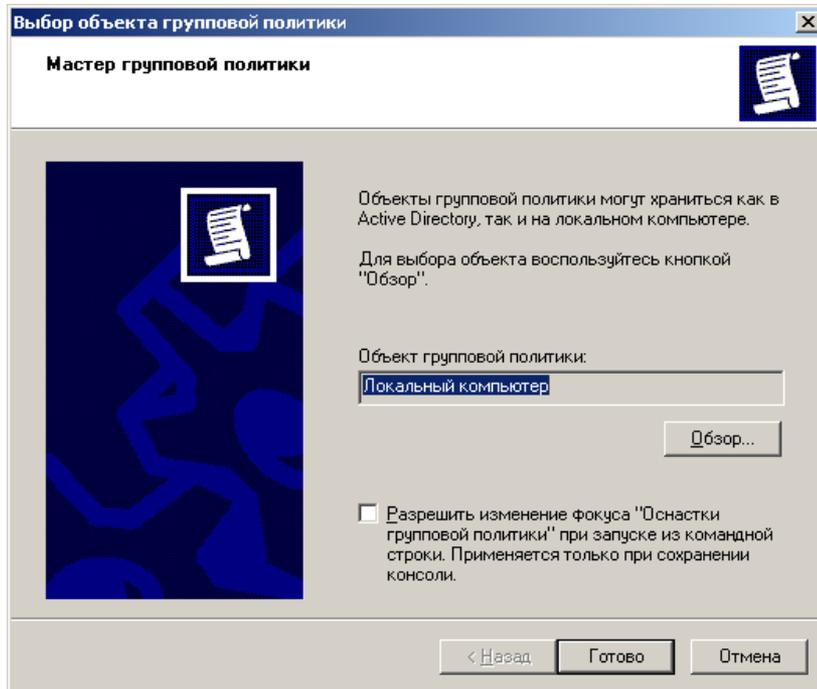
- Система размещает информацию о GPO в двух местах:
 - Значения всех атрибутов объектов размещаются в специальном контейнере групповой политик (Group Policy Container, GPC) Active Directory .
 - Для размещения файлов, связанных с применением групповых политик, система использует специальную структуру – **шаблон групповой политики**.
 - Данный шаблон представляет собой папку, которая располагается внутри папки SYSVOL\sysvol\\policies. По умолчанию папка располагается внутри системной папки Windows (Папка шаблонов групповой политики).
- Создание и удаление объектов групповой политики разрешено пользователям, являющимся членами групп безопасности **Администраторы домена и Администраторы предприятия**.

Создание объекта групповой политики

- Для создания объектов групповой политики используется специальная оснастка консоли управления Windows – **Редактор объектов групповой политики.**

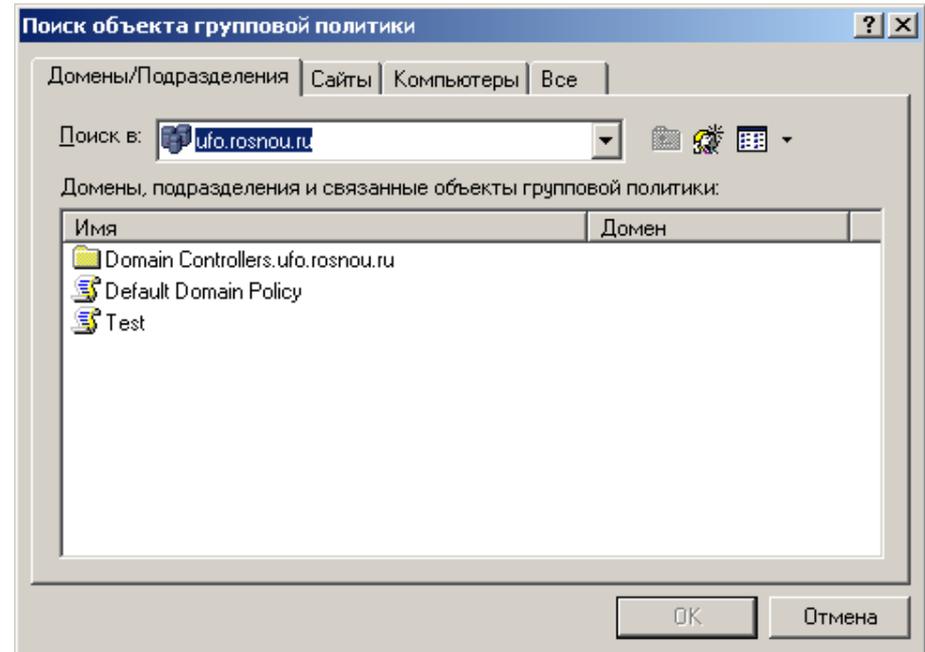


Создание объекта групповой политики



- Если есть необходимость создания нового объекта групповой политики, то используется специальная кнопка.

- В Мастере групповой политики выбрать в качестве объекта с помощью кнопки **Обзор** – Домен/Подразделение нужный объект.



Конфигурирование объектов групповой политики

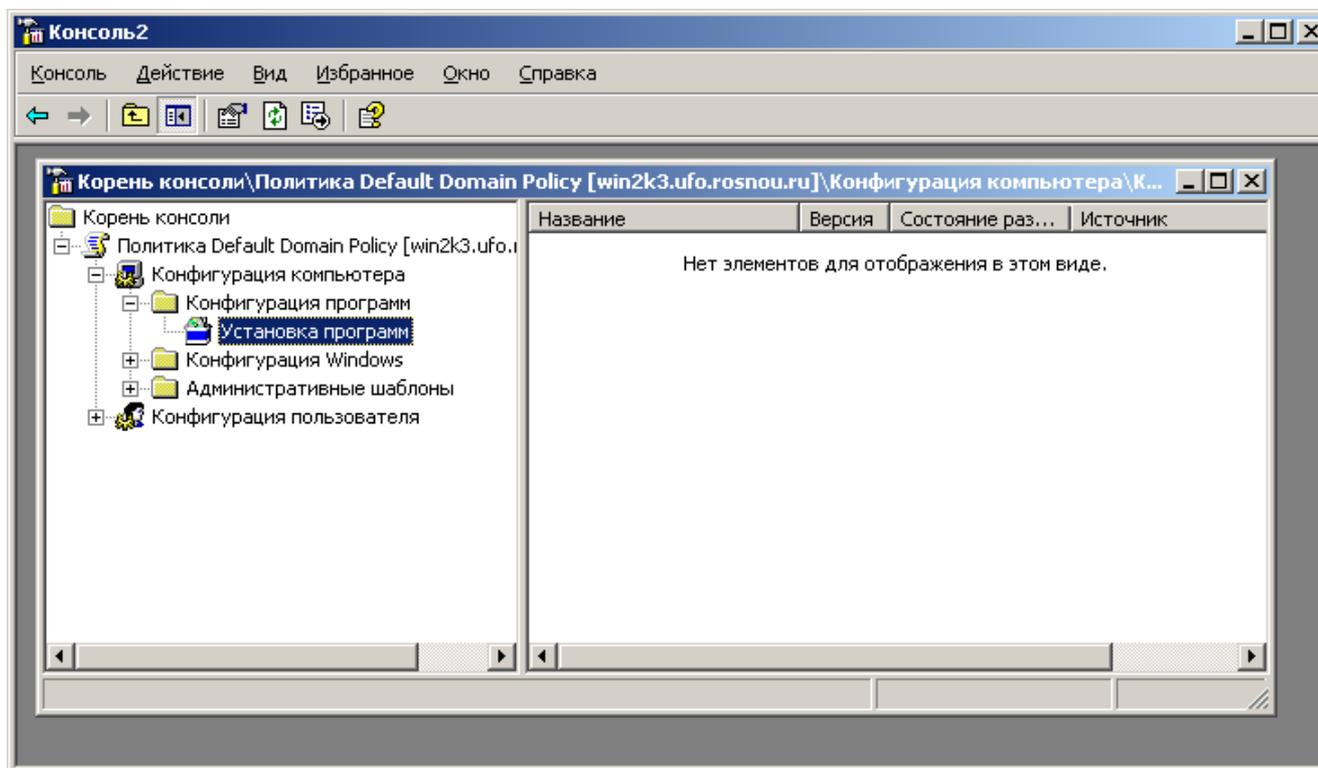
- Папка «Конфигурация пользователя» оснастки **Групповая политика** используется для задания политик, применяемых к пользователям независимо от того, какой компьютер используется для входа в систему.
 - Узел «Конфигурация пользователя» содержит элементы :
 - «Конфигурация программ»,
 - «Конфигурация Windows»,
 - «Административные шаблоны»,

Конфигурирование объектов групповой политики

- С помощью узла «Конфигурация компьютера» в оснастке **Групповая политика** можно устанавливать политики, применяемые к компьютерам, вне зависимости от того, кто работает на них.
 - Узел «Конфигурация компьютера» содержит подузлы:
 - «Конфигурация программ»,
 - «Конфигурация Windows»,
 - «Административные шаблоны».
- Редактор объектов групповой политики допускает добавление или удаление расширений.

Конфигурирование групповой ПОЛИТИКИ

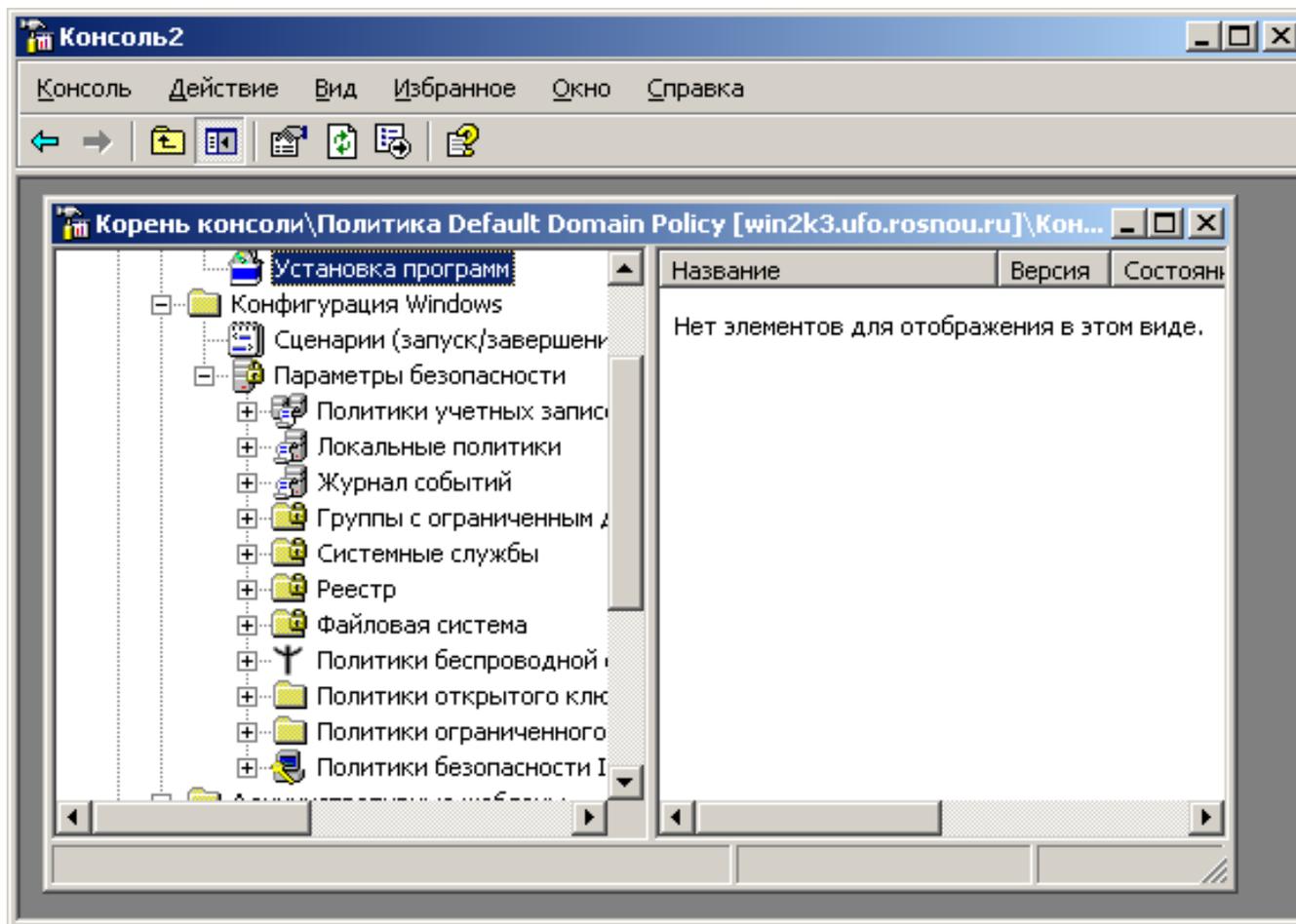
- Выделяются следующие уровни конфигурирования групповой политики:
 - **Конфигурация программ.** Здесь размещены расширения mmc, применяемые для конфигурирования параметров групповых политик:
 - **Установка программ.**



Конфигурирование групповой политики

- **Конфигурация Windows.**
- В данном контейнере размещаются расширения mmc, ответственные за управление конфигурацией системы.
- Содержимое контейнера различается для групповых политик пользователя или компьютера:
 - **Сценарии.** Определяются сценарии, которые будут выполняться при запуске/выключении компьютера (при входе/выходе пользователя в систему).
 - **Параметры безопасности.** В данном расширении выполняется управление параметрами групповой политики, связанными с функционированием системы безопасности. Часть параметров может быть определена с помощью других утилит.

Конфигурирование групповой политики



Конфигурирование Windows через GPO

▫ **Конфигурация Windows.**

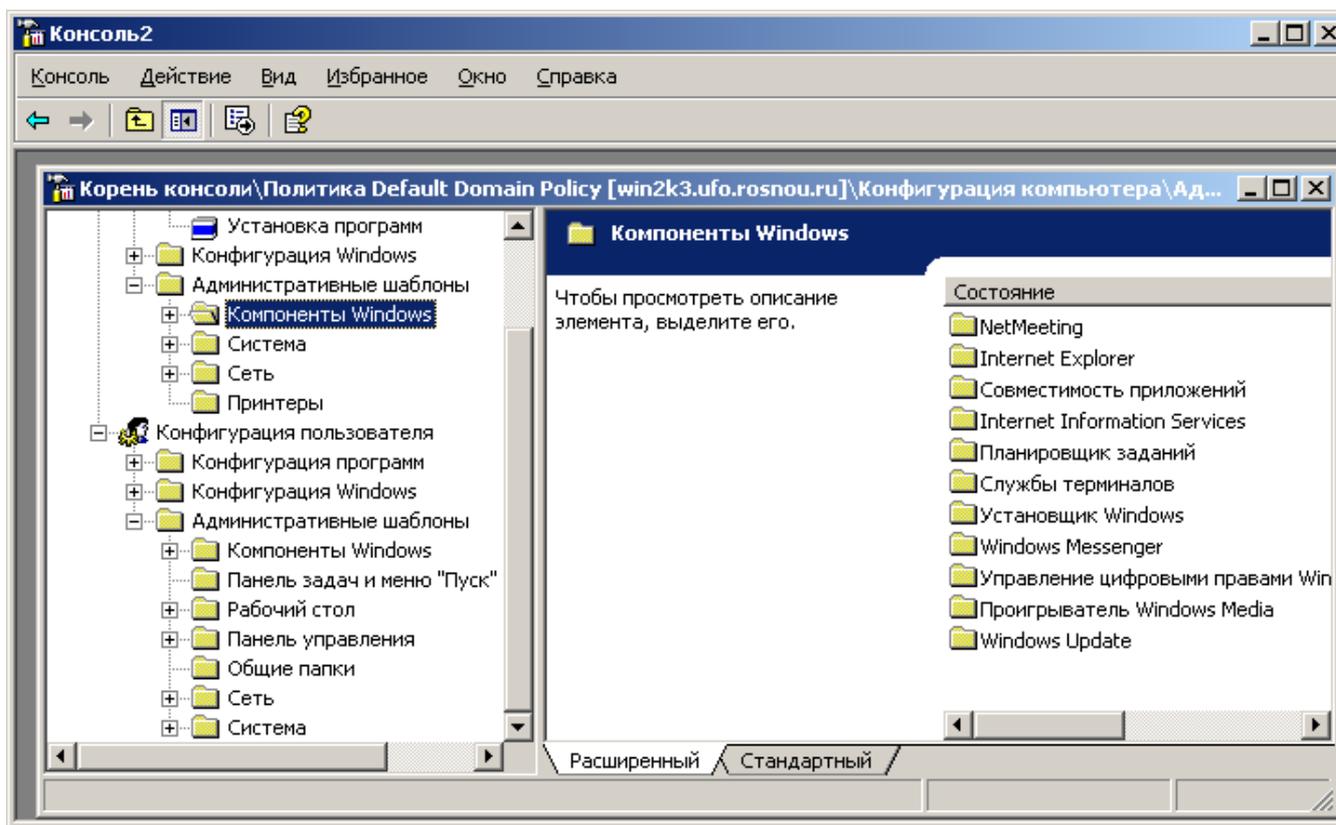
- **Службы удаленной установки.** Данное расширение используется для определения параметров удаленной установки на клиентском компьютере.
- **Настройка Internet Explorer.** Используется для конфигурирования Internet Explorer на компьютерах домена, работающих под управлением Windows XP/2000 или Server 2003.
- **Перенаправление папок.** С помощью данного расширения можно осуществлять перенаправление папок из пользовательского профиля в некоторый сетевой ресурс.

Сценарии входа, выхода, запуска и завершения работы

- **Редактор объектов групповой политики** включает в себя два расширения для развертывания сценариев:
 - **Сценарии (запуск/завершение)**. Это расширение, расположенное в узле дерева консоли редактора объектов групповой политики «Конфигурация компьютера\Конфигурация Windows», используется для указания сценариев, выполняемых при запуске и завершении работы компьютера.
 - Эти сценарии выполняются с правами локальной системы.
 - **Сценарии (вход/выход из системы)**. Это расширение, расположенное в узле дерева консоли редактора объектов групповой политики «Конфигурация пользователя\Конфигурация Windows», используется для указания сценариев, выполняемых при входе и выходе пользователя из системы.
 - Эти сценарии запускаются с правами пользователя, а не администратора.
- Операционные системы семейства Windows Server содержат сервер сценариев Windows:
 - Включена поддержка как сценариев Visual Basic Scripting Edition (файлы .vbs), так и сценариев и JScript (файлы .js).

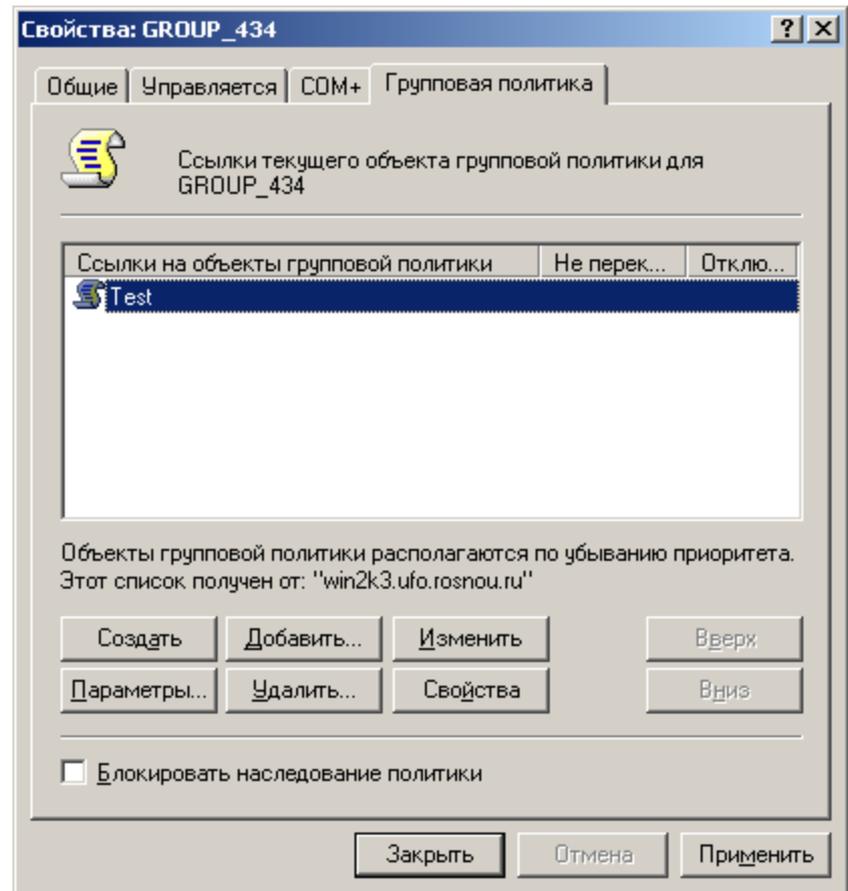
Шаблоны групповой политики

- **Административный шаблон.** Данный контейнер содержит параметры групповой политики, применяемые для управления содержимым системным реестром.



Применение групповой политики

- Для связывания объекта групповой политики с контейнером каталога используется административная оснастка **Active Directory – Пользователи и компьютеры**.
- Выбрав организационную единицу с помощью контекстного меню открывается закладка **Групповая политика**.



Группы безопасности и групповая политика

- Объекты групповой политики рассматриваются в качестве субъекта системы безопасности.
- Каждый объект имеет собственный дескриптор безопасности, который определяет атрибуты безопасности объекта, в том числе – избирательный список контроля доступа (DACL).

Анализ и настройка безопасности

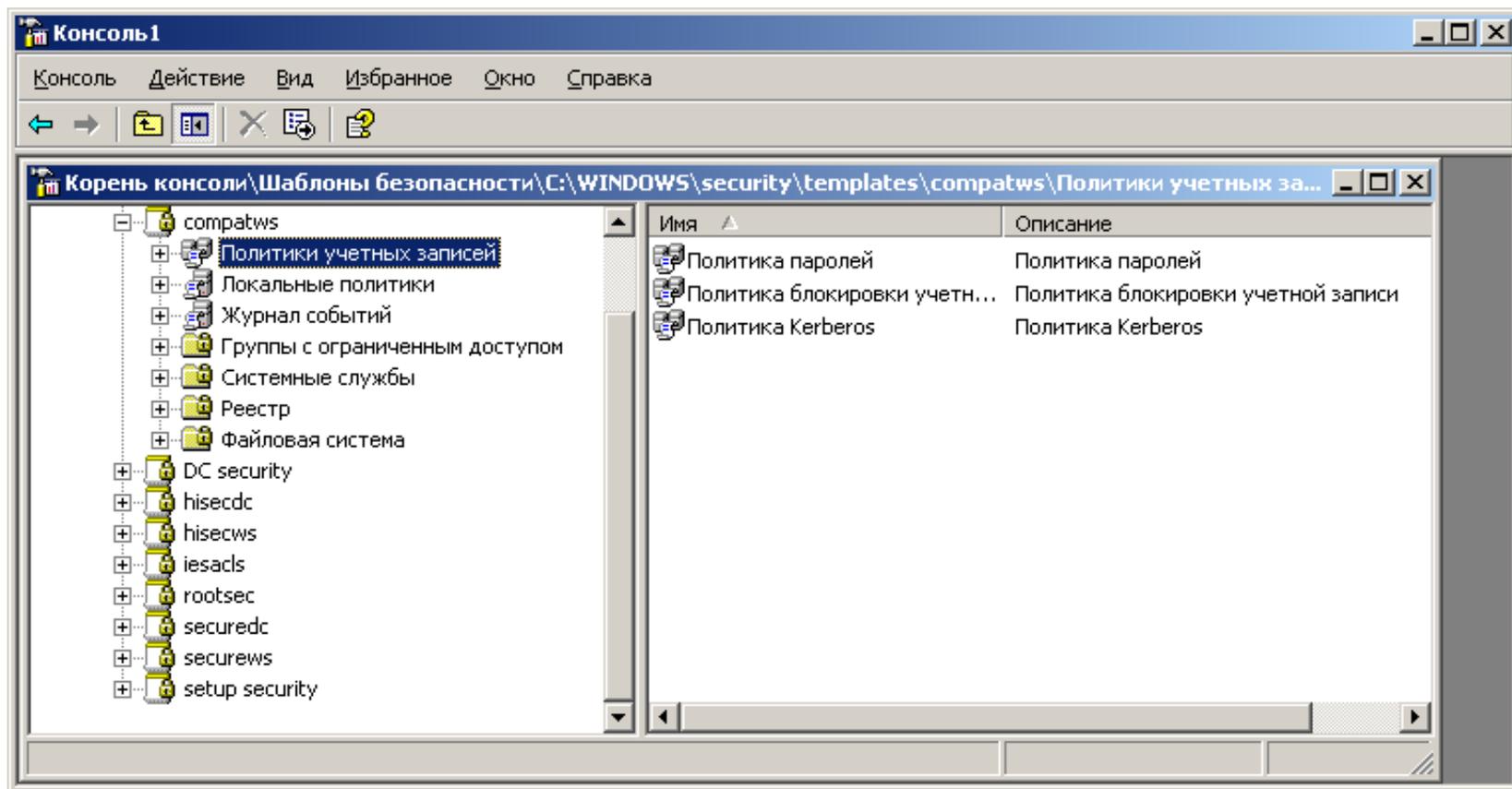
- Оснастка «Анализ и настройка безопасности» используется для анализа и настройки безопасности локального компьютера.

Средство управления настройкой безопасности	Описание
Шаблоны безопасности	Определение политики безопасности в шаблоне. Эти шаблоны могут применяться к групповой политике или к локальному компьютеру.
Расширение «Параметры безопасности» для групповой политики	Изменение отдельных параметров безопасности домена, узла или подразделения
Локальная политика безопасности	Изменение отдельных параметров безопасности локального компьютера.
Secedit	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.
- **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.

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`

Выводы

- Операционные системы семейства Windows обладают усовершенствованными технологиями управления конфигурацией пользователей и компьютеров, входящих в домен.
- Использование механизмов групповых политик позволяет администраторам настроить среду работы пользователя, организовать конфигурирование пользовательских приложений, обеспечить выполнение выбранной политики безопасности.
- Групповые политики могут быть использованы для управления конфигурациями отдельных пользователей, групп пользователей и компьютеров в рамках домена Windows.
- Допускается механизм наследования выработанных политик в рамках леса.

Выводы

- Параметры политики хранятся в объектах групповой политики.
- Редактор объектов групповой политики можно рассматривать как приложение, типом документов которого является объект групповой политики, так же как текстовый редактор использует файлы .doc или .txt.
- Существует два типа объектов групповой политики: локальные и нелокальные.
 - **Локальные объекты групповой политики** хранятся на локальном компьютере. На компьютере существует только один локальный объект групповой политики, содержащий набор параметров, доступных в нелокальном объекте групповой политики. В случае конфликта параметры локального объекта будут перезаписаны нелокальными параметрами или применены совместно.
 - **Нелокальные объекты групповой политики** хранятся на контроллере домена и доступны только в среде Active Directory. Они применяются к пользователям или компьютерам в сайте, домене или подразделении, связанном с объектом групповой политики.

Выводы

- В общем случае групповая политика передается от родительских контейнеров к дочерним в домене, который можно просмотреть с помощью оснастки Active Directory — пользователи и компьютеры.
- Групповая политика не наследуется от родительских доменов к дочерним, например от веб-узла wingtiptoys.com к узлу sales.wingtiptoys.com.
- На каждом компьютере Windows имеется по крайней мере один локальный объект групповой политики.
- Объекты групповой политики в отличие от локальных объектов этой политики являются виртуальными. Сведения о параметрах политики для GPO фактически хранятся в двух расположениях: **в контейнере** и **в шаблоне групповой политики**.
 - **Контейнер групповой политики** представляет собой объект службы каталогов. Он состоит из субконтейнеров для хранения сведений о групповой политике пользователя и компьютера.
 - **Шаблон групповой политики** — это папка контроллеров домена для хранения домена объекта групповой политики.