Лекция # 5

ШАБЛОНЫ БЕЗОПАСНОСТИ

Удалённое управление рабочей станцией

Active Directory – пользователи и компьютеры -> … -> <Объект Компьютер> -> Управление

Администраторы домена \Администратор -> локальных администраторов

Возможности удалённого управления

Просмотр событий
Сведения о системе
Диспетчер устройств
Управление дисками
Службы

Управление пользователями

Создание, удаление, задание атрибутов пользователей и групп
Завершение сеанса
    с закрытием приложений
    без закрытия
Перезагрузка

Возможности net use

NET USE [имя_устройства | *]
[\\имя_компьютера\имя_ресурса[\том] [пароль | *]]
[/USER:[имя_домена\]имя_пользователя]
[/USER:[имя_домена_с_точками\]
имя_пользователя]

[/USER:[имя_пользователя@имя_домена_с_точками]
[[/DELETE] | [/PERSISTENT:{YES | NO}]]

net use k: \\CN\c$ /user:Администратор

Скрытые общие ресурсы

IPC$ - канал для установления связи
ADMIN$ (C:\WINNT)
<имя локального стационарного диска>$ (C$, …)

Создание общих ресурсов

Использование дискового пространства рабочей станции
Удалённое назначение сетевых разрешений
Возможность удалённого редактирования локального профиля пользователя или локальной копии перемещаемого

Файловая система

- Удалённое и групповое управление разрешениями локальных файловых систем
- Действуют наследование и приоритеты
- Играет роль последовательность применения ОГП, для записей внутри ОГП существенны запреты изменения
- Применение на этапе загрузки компьютера/принудительное/фоновое обновление групповой политики

Файловая система

- Запрет изменения разрешений (групповой политикой)/настройка разрешений
- Настройка наследования от родительских объектов
- Распространение на дочерние объекты со слиянием/с заменой
- Настройка аудита аналогична
- Невозможность замены владельца

Фоновое обновление ГП

1) Разрешить: отключить запрещение

2) Установить интервал обновления и интервал добавляемой случайной величины
DC/usual computer; 0 мин ~ 7 секунд
3) Асинхронное применение ГП
4) Способ замыкания на себя

Дополнительные параметры ГП

5) соединения; фоновое периодическое обновление; принуждение:

- Реестр
- Internet Explorer
- Установка программ
- Перенаправление папок
- Сценарии
- Безопасность
- IP-безопасность
- EFS-шифрование
- Дисковые квоты

Принудительное обновление ГП

Secedit

- анализ настроек безопасности системы;
- применение шаблонов безопасности;
- перезагрузка политики безопасности;
- экспорт политики безопасности в файл шаблона.

Группы с ограниченным доступом

Фиксированный состав пользователей (производится как добавление, так и удаление)

Ограничение снизу по членству самой группы в других группах

Реестр

Настройка доступа к разделам реестра
Наследование, приоритеты
Порядок применения ОГП
Аналогично файловой системе
regedit
regedt32

Системные службы

Удалённое управление локальными службами
Режим запуска (автоматически, вручную, запрещён)
Настройка безопасности: пользователи, группы пользователей, суммирование прав, приоритеты

Дисковые квоты

Включение
Запрет на использование большего пространства
Значения по умолчанию: порог отключения и предупреждения
Аудит превышения порогов
Применения к съёмным носителям

Политика паролей и входа

Минимальный/максимальный срок действия
Минимальная длина
Требования к сложности
Неповторяемость
Шифрование
Число попыток до блокировки
Сброс счётчика блокировки
Время блокировки

Панель управления

Скрыть всю/отдельные элементы
Показать отдельные элементы
Добавление/удаление программ
- скрыть *изменить/удалить*
- скрыть *добавить*
- *скрыть добавить с CD-ROM\из сети, Microsoft*

Меню Пуск

Скрыть Windows Update
Скрыть Помощь
Скрыть Выполнить
Скрыть Поиск
Добавить/скрыть Завершение сеанса
Скрыть Диспетчер задач
Запретить Завершение работы
Запрет контекстного меню панели задач
Не хранить историю документов
Запрет персонального меню

Рабочий стол

Убрать все пиктограммы
Убрать Мои документы
Убрать контекстное меню Мои документы
Убрать контекстное меню Мой компьютер
Убрать Моё сетевое окружение
Убрать IE
Запретить менять расположение папки Мои документы
Запретить изменение панелей в панели задач
Обязательно Active Desktop

Рабочий стол

Обязательный фон рабочего стола Active Desktop
Запрет изменения, добавления, удаления элементов
Запрет закрытия элементов

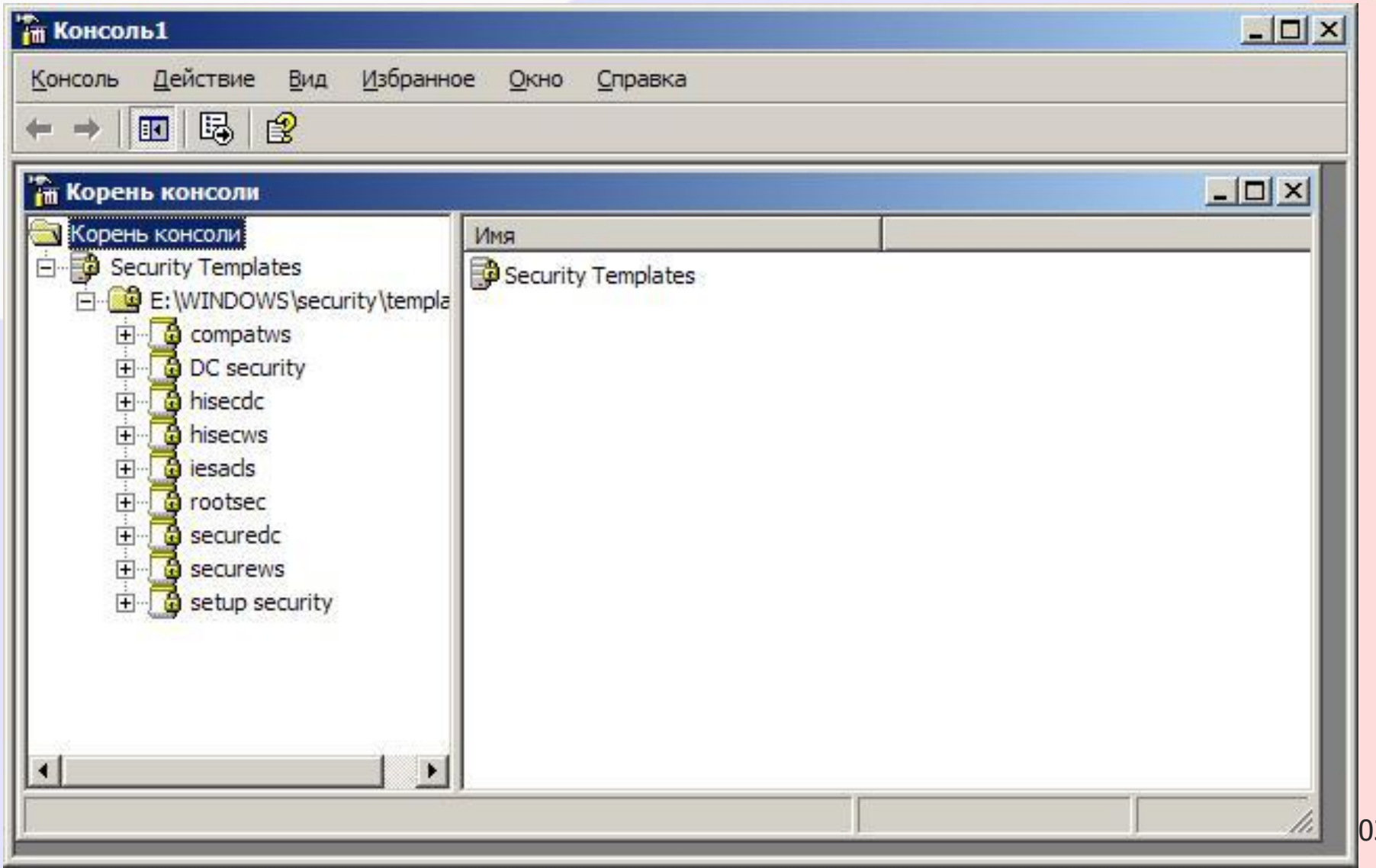
Административные шаблоны

*.adm
Набор записей в реестре
Возможность подключения и отключения
Возможность самостоятельного редактирования и создания

Шаблоны безопасности

*.inf
Возможность анализа при помощи утилиты
Анализ на предмет соответствия определённому уровню безопасности
Выявление узких мест
Стандартные поставляемые файлы для различных уровней безопасности

Управление Шаблонами безопасности



Список шаблонов и их краткое описание

Шаблон	Редакция Windows 2000	Описание
basicdc	Server	Параметры безопасности по умолчанию для контроллеров домена. Не содержит специальных ограничений на файлы, папки и разделы реестра
basicsv	Server	Параметры безопасности по умолчанию для серверов. Не содержит специальных ограничений на файлы, папки и разделы реестра

basicwk	все	Параметры безопасности по умолчанию для рабочих станций. Не содержит специальных ограничений на файлы, папки и разделы реестра
compatws	все	Содержит только настройки разрешений по умолчанию для файлов, папок и разделов реестра
DC security	Server	Параметры безопасности по умолчанию, используемые при установке Active Directory на Windows Server 2003

hisecdc	Server	Содержит дополнительные параметры безопасности для контроллеров домена. Включает все параметры шаблона **securedc**
hisecws	все	Содержит дополнительные параметры безопасности для рабочих станций. Вводит ограничения для группы опытных пользователей и сервера терминалов. Включает все параметры шаблона **securews**
notssid	Server	Удаляет идентификатор безопасности пользователя сервера терминалов из всех разрешений и групп, блокируя тем самым этому пользователю доступ к компьютеру
ocfiless	Server	Содержит дополнительные параметры безопасности для файлов необязательных компонентов

ocfilesw	все	Содержит дополнительные параметры безопасности для файлов необязательных компонентов
securedc	Server	Специальные разрешения для файлов, папок и реестра контроллера домена. Отключение "лишних" служб, защита прочих областей
securews	все	Специальные разрешения для файлов, папок и реестра рабочей станции. Отключение "лишних" служб, защита прочих областей
setup security	все	Параметры безопасности, задаваемые на любом компьютере Windows во время установки