

Администрирование Windows Server 2012

Лабораторная работа № 6. Групповые политики

Часть 1: Групповые политики

Групповая политика — это компонент Windows, который позволяет централизованно управлять конфигурацией пользователей и компьютеров в домене Active Directory. Вместо того чтобы настраивать каждый компьютер вручную, администратор определяет параметры в одном месте, и они автоматически применяются ко всем целевым объектам.

Групповая политика обеспечивает инфраструктуру, в которой можно централизованно определять и развертывать пользователей и компьютеры на предприятии. В среде, управляемой четко определенной инфраструктурой групповой политики, непосредственная конфигурация рабочих столов практически не выполняется. Вся конфигурация определяется, внедряется и обновляется с помощью параметров объектов групповой политики GPO (Group Policy Object), которые управляют структурами предприятия, как, например, сайты, домены, а также отдельные подразделения и группы.

Групповая политика представляет собой компонент Windows, который позволяет управлять изменениями и конфигурацией пользователей и компьютеров в центральной точке администрирования.

Параметры политики: Групповая политика основана на отдельных *параметрах политики* (они также называются *политиками*) и определяют конкретную конфигурацию для применения. Например, существует параметр политики, запрещающий пользователю получать доступ к средствам редактирования реестра. Если определить этот параметр политики и применить его к пользователю, то пользователь не запустит такие инструменты, как редактор реестра Regedit.exe. Еще один параметр политики, позволяющий отключить локальную учетную запись Администратор (Administrator), применяется, к примеру, для отключения учетной записи администратора на всех настольных системах и ноутбуках пользователей.

Эти два примера определяют важный момент: некоторые параметры политики влияют на пользователя независимо от компьютера, на котором пользователь входит в сеть, а другие параметры политики влияют на компьютер независимо от пользователя, который входит на этот компьютер. Такие параметры политики, как параметр, запрещающий доступ к средствам редактирования реестра, называются *параметрами конфигурации пользователей*, или *параметрами пользователей*. Параметр политики, отключающий учетную запись администратора, а также другие аналогичные параметры, применяемые к компьютеру, называются *параметрами конфигурации компьютеров*, или *параметрами компьютеров*.

Объекты групповой политики: Параметры политики определяются и содержатся в объекте групповой политики GPO (Group Policy Object). Объект GPO включает один или множество параметров политики и, следовательно, применяется к одному или множеству конфигураций пользователя или компьютера.

Параметр политики может пребывать в трех состояниях: Не задан (Not Configured), Включен (Enabled) и Отключен (Disabled).

Конфигурация определяется параметрами в объектах групповой политики. Однако изменения конфигурации в GPO не влияют на компьютеры или пользователей предприятия, если к ним не применяется объект GPO. Эта концепция называется *областью действия* объекта групповой политики. Область действия GPO представляет собой коллекцию пользователей и компьютеров, к которым применяются параметры GPO.

Для управления областью действия GPO используется несколько методов. Основной метод состоит в связывании GPO. Объекты GPO можно связать с сайтами, доменами и подразделениями в Active Directory. После этого сайт, домен или подразделение определяют пределы области действия GPO. Параметры политики, определенные в GPO, будут влиять на все компьютеры и пользователей внутри узла, домена или подразделения, включая дочерние подразделения. Один объект GPO можно привязать к множеству сайтов или подразделений.

Затем область действия GPO можно ограничить дополнительно с помощью *фильтров безопасности*, указывающих на глобальные группы безопасности, к которым должен применяться или не применяться объект GPO, или *фильтров инструментария управления Windows* (Windows Management Instrumentation), указывающих область действия с помощью таких характеристик системы, как номер версии или свободное дисковое пространство.

Отдельный пользователь или компьютер может подпадать под область действия множества объектов GPO, привязанных к сайтам, домену или подразделениями, где расположен пользователь или компьютер. Таким образом, в случае применения множества объектов GPO параметры политики могут конфигурироваться иначе. Поэтому нужно оцепить *Результирующую политику RSoP* (Resultant Set of Policy), определяющую параметры, которые будут применены к клиенту в случае использования множества объектов GPO.

Упражнение 1. Создание, редактирование и определение области действия объекта групповой политики

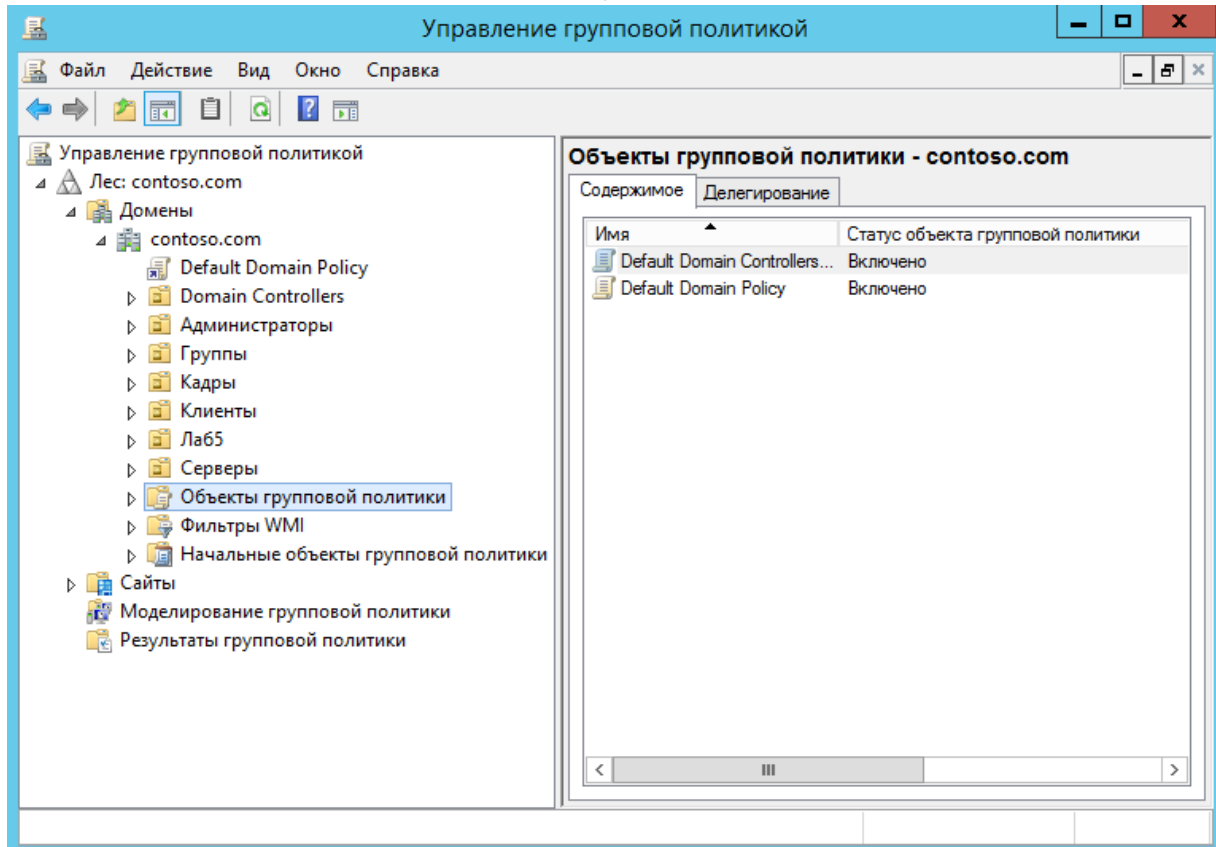
Создайте объект GPO, который реализует параметр обязательной политики безопасности Contoso, Ltd с областью действия для всех пользователей и компьютеров в домене.

1. Войдите на машину SERVER01 как администратор.

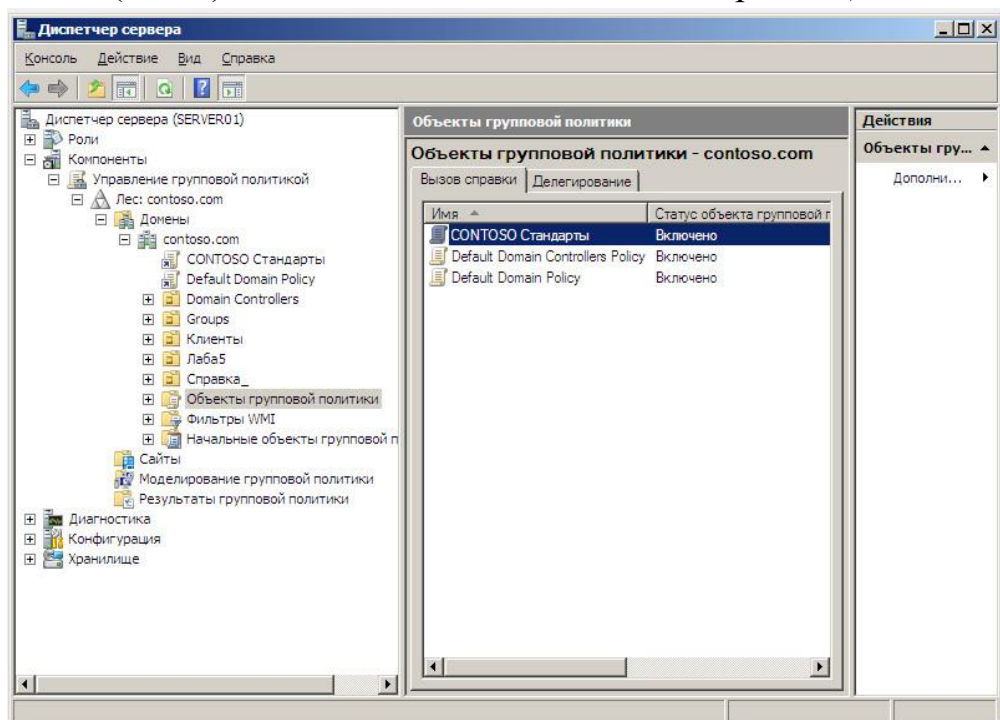
2. В группе Администрирование откройте консоль Управление групповой политикой.

3. Разверните лес и домен contoso.com и откройте контейнер Объекты групповой политики.

4. В дереве консоли щелкните правой кнопкой мыши контейнер Объекты групповой политики и выполните команду Создать (New).



5. В поле Имя (Name) введите имя CONTOSO Стандарты. Щелкните ОК.



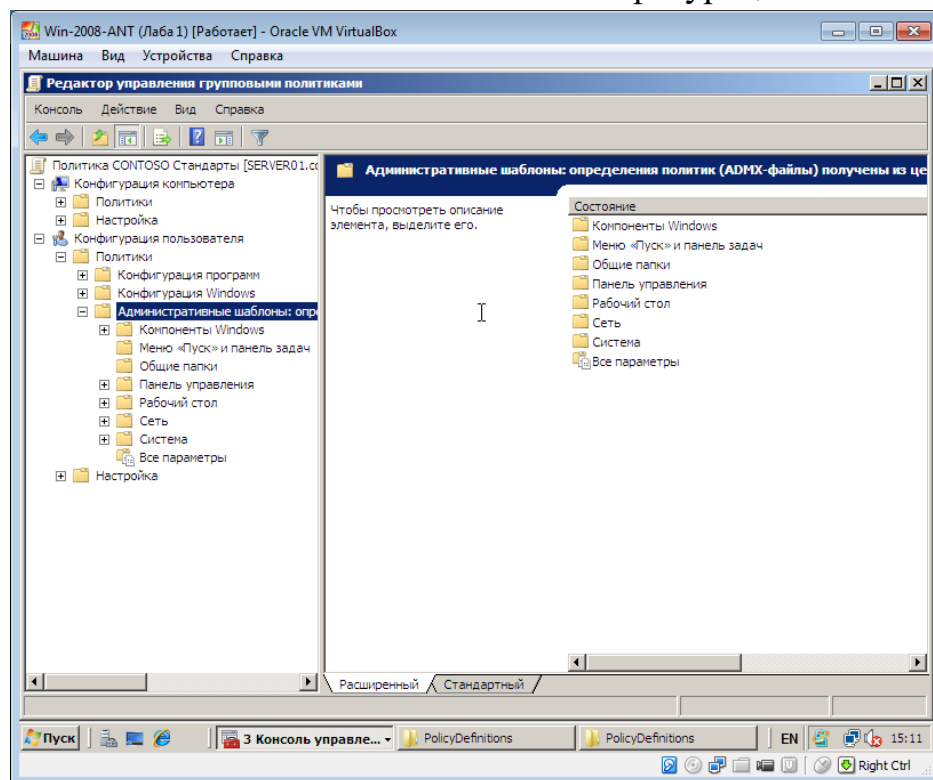
6. Щелкните правой кнопкой мыши объект CONTOSO Стандарты и выполните команду Изменить (Edit). Откроется Редактор управления групповыми политиками.

7. В консоли щелкните правой кнопкой мыши корневой узел CONTOSO Стандарты и выполните команду Свойства (Properties).

8. Перейдите на вкладку Комментарий (Comment) и введите комментарий «Стандарты корпоративных политик Contoso. Параметры влияют на всех пользователей и компьютеры в домене. Ответственное лицо за объект GPO: ваше имя». Щелкните ОК. В этом сценарии корпоративная политика безопасности Contoso указывает, что компьютеры нельзя оставлять без присмотра и входить на них после 10 мин. простоя. Для того чтобы выполнить это требование, конфигурируется время ожидания экранной заставки и параметры политики пароля защиты экранной заставки. Для локализации этих параметров политики применяются новые поисковые возможности Windows Server 2012.

9. Разверните узел Конфигурация пользователя\Политики\Административные шаблоны (User Configuration\Policies\Administrative Templates).

10. Просмотрите параметры в этом узле. Прочитайте описание интересующих вас параметров политики. Не вносите изменения в конфигурацию.

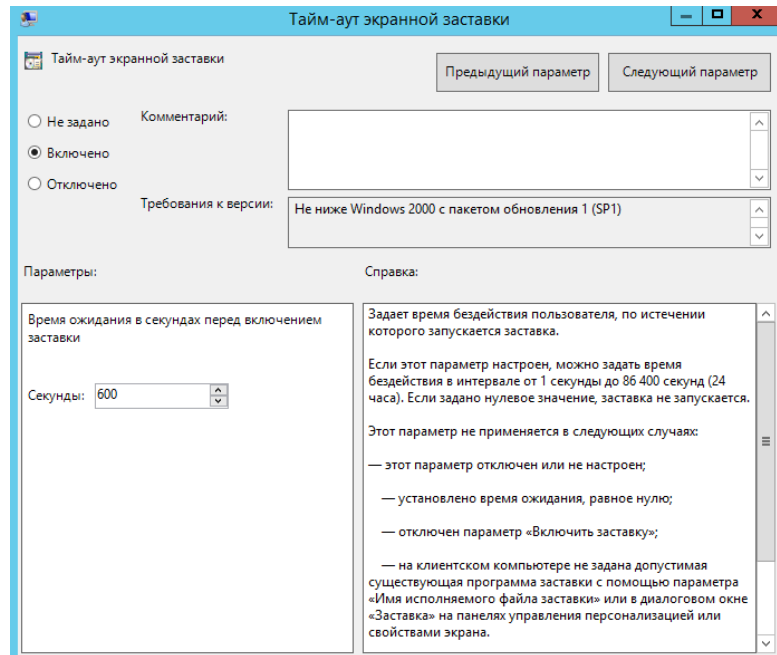


11. В узле Панель управления\Персонализация щелкните параметр политики Тайм-аут экранной заставки. В левой части панели сведений консоли отобразится описание параметра.

12. Дважды щелкните параметр политики Тайм-аут экранной заставки.

13. Выберите опцию **Включено**.

14. В поле Секунды введите значение 600.



15. В поле Комментарий введите «Корпоративная политика безопасности реализована с помощью этой политики в комбинации с парольной защитой экранной заставки». Щелкните ОК.

16. Дважды щелкните параметр политики Защита заставки с помощью пароля

17. Выберите опцию Включено.

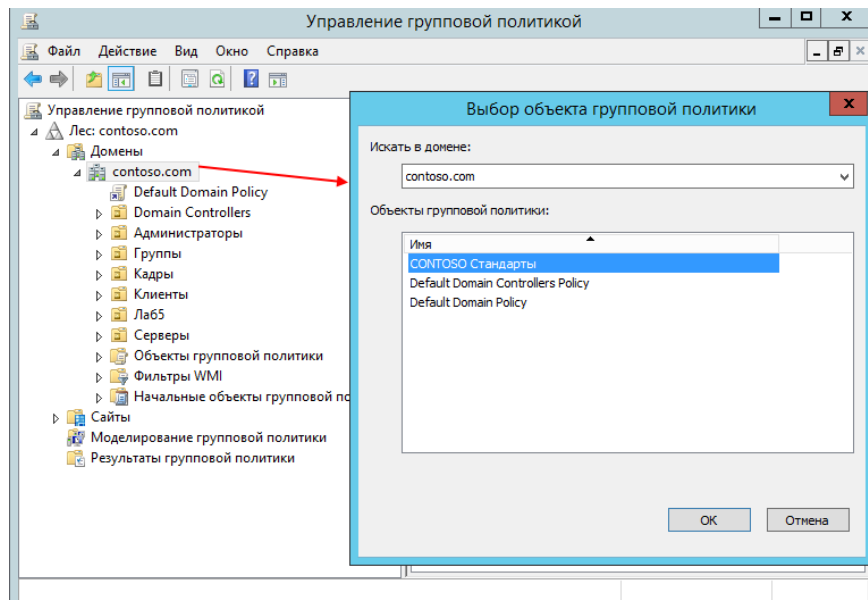
18. На вкладке Комментарий введите «Корпоративная политика безопасности реализована с помощью этой политики в комбинации с политикой тайм-аута экранной заставки». щелкните ОК.

19. Закройте редактор Управления групповой политики (GPO).

Изменения, внесенные в GPME, сохраняются в реальном времени. Такая команда, как Сохранить (Save), отсутствует.

20. В консоли Управление групповой политикой щелкните правой кнопкой мыши домен contoso.com и выполните команду Связать существующий объект GPO.

21. Выберите объект групповой политики CONTOSO Стандарты и щелкните ОК.



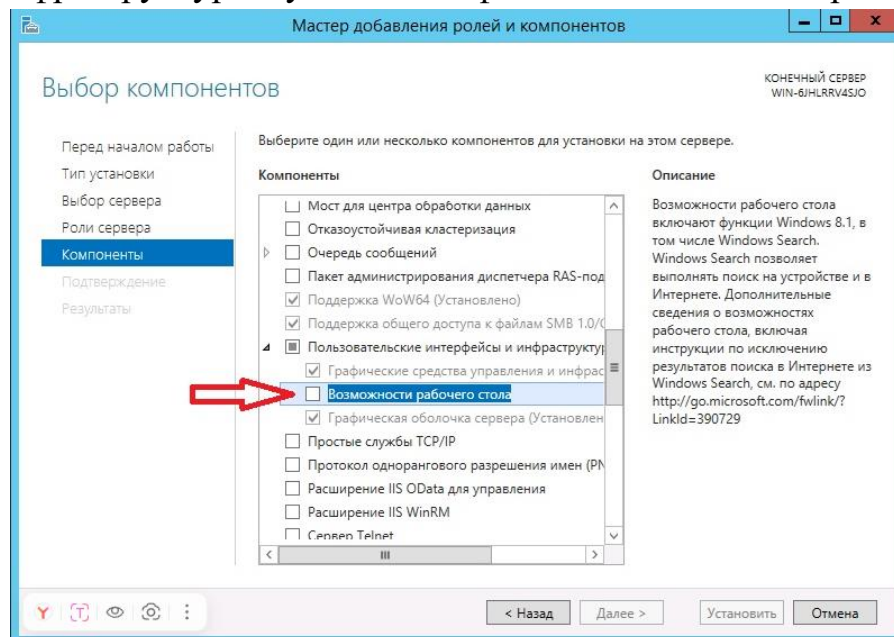
Упражнение 2. Просмотр результатов применения групповой политики

Проверьте результат применения параметра групповой политики, отконфигурированного в упражнении 1, а также попрактикуйтесь в обновлении политики вручную с помощью инструмента Gpupdate.exe.

1. В Windows Server 2012 пункт «Персонализация» по умолчанию отсутствует в контекстном меню рабочего стола, поскольку это серверная операционная система, где GUI-функции рабочих станций не устанавливаются автоматически.

2. Откройте Диспетчер сервера → Управление → Добавить роли и компоненты.

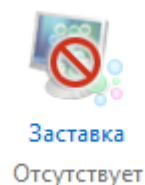
3. На странице Выбор компонентов разверните раздел Пользовательские интерфейсы и инфраструктура и установите флажок Возможности рабочего стола



4. При появлении запроса на установку дополнительных требуемых компонентов нажмите **Добавить компоненты**.

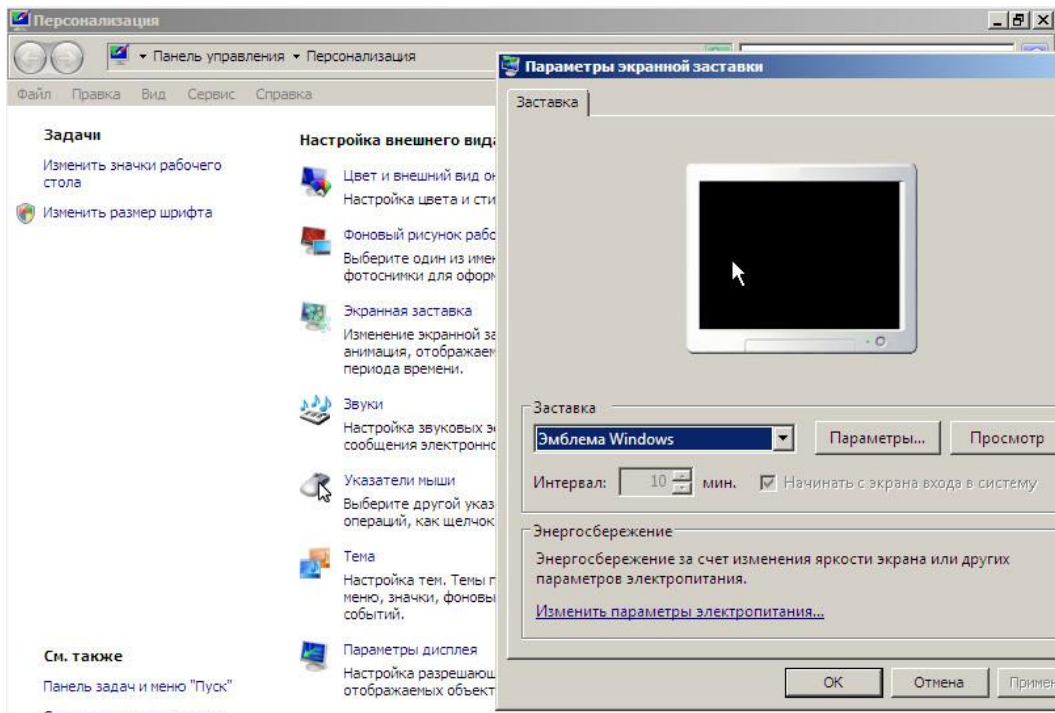
5. Завершите установку и перезагрузите сервер. После перезагрузки пункт «Персонализация» станет доступен в контекстном меню рабочего стола.

6. Откройте Персонализацию и Щелкните ссылку Заставка.



7. Теперь вы не сможете изменить время ожидания и отображение экранной заставки.

(Примечание, единицы измерения минуты – секунды)

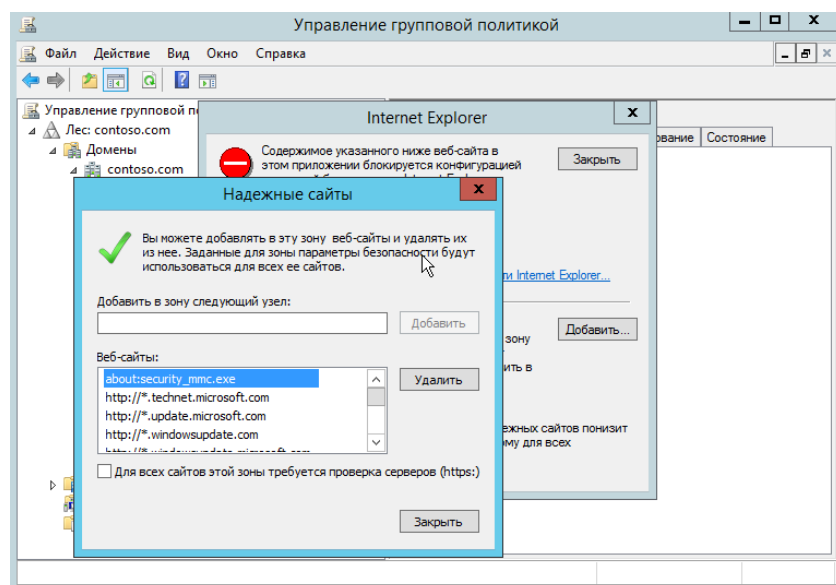


Упражнение 3. Обзор объекта групповой политики

Просмотрев результаты применения GPO, проанализируйте сам объект GPO, чтобы лучше понять принцип внутренней работы групповой политики.

1. В контейнере Объекты групповой политики консоли Управление групповой политикой выберите объект CONTOSO Стандарты.
2. В секции Связи вкладки Область показаны связи GPO.
3. Перейдите на вкладку Параметры, чтобы просмотреть отчет о параметрах в объекте GPO.

Если включена конфигурация повышенной безопасности Internet Explorer, подтвердите добавление содержимого веб-узла *about:security_mmc.exe* в зону надежных узлов.



4. Щелкните ссылку Показать все (Show All) в верхней части отчета, чтобы развернуть все секции отчета. Как видите, в отчет добавлены комментарии к параметрам политики.

CONTOSO Стандарты

Область

Сведения

Параметры

Делегирование

Состояние

CONTOSO Стандарты

Данные собраны: 27.07.2026 19:44:20

Конфигурация компьютера (включено)

Параметры не заданы.

Конфигурация пользователя (включено)

Политики

Административные шаблоны

Панель управления/Персонализация

Определения политик (ADMX-файлы) получены с локального компьютера.

Политика	Параметр	Примечание
Защита заставки с помощью пароля	Включено	Корпоративная политика безопасности реализована с помощью этой политики в комбинации с политикой тайм-аута экранной заставки
Тайм-аут экранной заставки	Включено	Корпоративная политика безопасности реализована с помощью этой политики в комбинации с парольной защитой экранной заставки.

Время ожидания в секундах перед включением заставки

Секунды:

600

5. Наведите указатель мыши на имя политики Тайм-аут экранной заставки (Screen Save Timeout). Как видите, оно представляет собой гиперссылку. Щелкните ее, чтобы просмотреть объяснение данного параметра политики.

6 Перейдите на вкладку Сведения, где отображаются ваши комментарии к объекту GPO вместе с информацией о номерах версии GPO.

7. Запишите уникальный код (Unique ID), отображаемый на вкладке Таблица (Details).

CONTOSO Стандарты

Область

Сведения

Параметры

Делегирование

Состояние

Домен:

contoso.com

Владелец:

Администраторы домена (CONTOSO\Администраторы домена)

Создан:

27.07.2026 18:01:14

Изменен:

27.07.2026 18:42:48

Версия пользователя:

2 (AD), 2 (SYSVOL)

Версия компьютера:

0 (AD), 0 (SYSVOL)

Уникальный код:

{202451D9-5584-4A02-9400-A7D5A5003A03}

Состояние GPO:

Включено

Комментарий:

Стандарты корпоративных политик - Contoso

8. Откройте папку \\contoso.com\SYSVOL\contoso.com\Policies.

9. Дважды щелкните папку с именем, которое соответствует уникальному коду объекта GPO.

Эта папка представляет шаблон GPT объекта GPO.

Упражнение 4. Создание центрального хранилища

Административные шаблоны (ADMX/ADML) определяют, какие параметры отображаются в редакторе групповых политик. По умолчанию каждый компьютер использует локальные шаблоны из папки %SystemRoot%\PolicyDefinitions. Чтобы все администраторы видели одинаковые шаблоны, их помещают в **центральное хранилище** — папку PolicyDefinitions в SYSVOL. Это гарантирует единообразие настроек на всех компьютерах в домене

Создайте центральное хранилище административных шаблонов для централизации управления шаблонами.

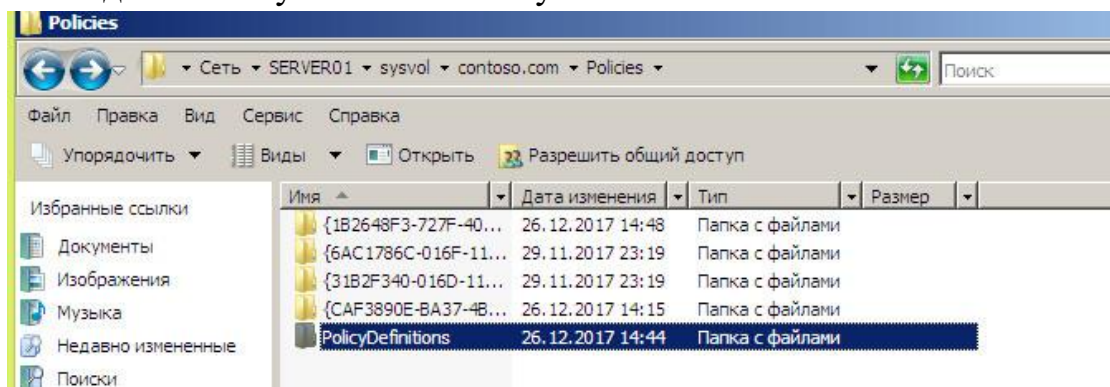
1. В консоли Управление групповой политикой щелкните правой кнопкой мыши объект групповой политики CONTOSO Стандарты и выполните команду Изменить (Edit).

2. Разверните узел Конфигурация пользователя\Политики\Административные шаблоны

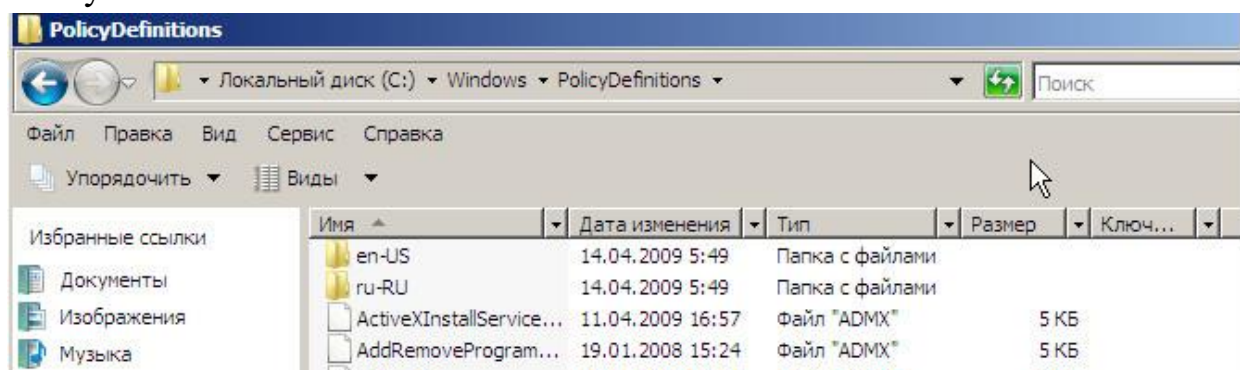
3. Отметьте: в имени узла указано, что Определения политик (ADMX-файлы) получены с локального компьютера. Закройте Редактор GPME.

5. Откройте папку \\contoso.com\SYSVOL\contoso.com\Policies.

6. Создайте папку с именем PolicyDefinitions.



7. Скопируйте в созданную папку содержимое папки %SystemRoot%\PolicyDefinitions.



8. В консоли Управление групповой политикой (Group Policy Management) щелкните правой кнопкой мыши объект CONTOSO Стандарты и выполните команду Изменить (Edit).

9. Разверните узел Конфигурация пользователя\Политики\Административные шаблоны.

10. В строке состояния/заголовке узла будет указано:

- до создания хранилища — что определения получены с **локального компьютера**;
- после — что определения получены **из центрального хранилища**.

Если после копирования всё ещё отображается «локальный компьютер», закройте и снова откройте GPME (или обновите консоль) — кэш шаблонов сбрасывается при перезапуске оснастки.

Закрепление материала

Задание 1. Запрет доступа к командной строке для группы «Аудиторы»

Создать GPO, который запрещает запуск командной строки (cmd.exe) для пользователей, входящих в группу «Аудиторы». Сотрудникам отдела аудита не требуются административные инструменты, и для безопасности их доступ к командной строке должен быть ограничен.

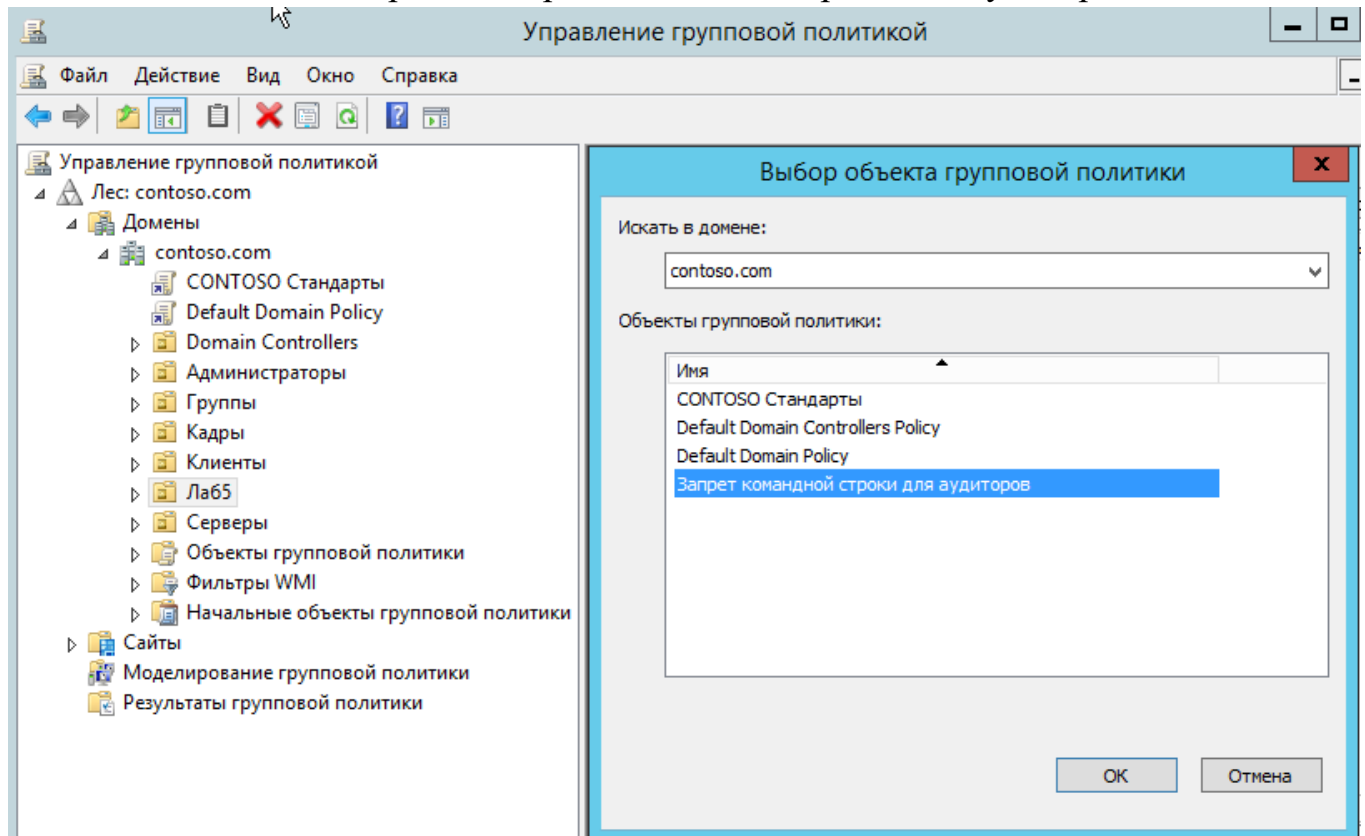
1. Войдите на машину SERVER01 под учетной записью Administrator.
2. Откройте консоль «Управление групповой политикой»:
3. В дереве консоли разверните: Лес: contoso.com → Домены → contoso.com
4. Щелкните правой кнопкой мыши контейнер «Объекты групповой политики» и выберите «Создать».
5. В поле «Имя» введите: Запрет командной строки для аудиторов. Нажмите ОК.
6. Щелкните правой кнопкой мыши созданный GPO «Запрет командной строки для аудиторов» и выберите «Изменить».
7. В редакторе GPO разверните путь: Конфигурация пользователя → Политики → Административные шаблоны → Система
8. Дважды щелкните параметр «Запретить доступ к командной строке».
9. Выберите вариант «Включено».
10. В поле «Запретить обработку сценариев в командной строке» выберите: Да
11. Перейдите на вкладку «**Комментарий**» и введите: Запрещает запуск командной строки для пользователей группы Аудиторы. Применяется в рамках политики безопасности. Нажмите ОК.
12. В консоли «Управление групповой политикой» выберите созданный GPO.
13. На вкладке «Область» (Scope) в секции «Фильтры безопасности»: Выделите группу «Прошедшие проверку» и нажмите кнопку «Удалить».

14. Нажмите кнопку «Добавить».

15. В поле «Введите имена выбираемых объектов» введите: Аудиторы

16. В дереве консоли найдите подразделение, в котором находятся пользователи (например, Лаб5). Щелкните правой кнопкой мыши по подразделению и выберите «Связать существующий объект GPO».

17. В списке выберите «Запрет командной строки для аудиторов».



18. Нажмите ОК.

19. Примените групповую политику к текущему компьютеру. Для этого откройте командную строку от имени администратора и выполните: `gpupdate /force`

20. Войдите на клиентский компьютер (SERVER02) под учетной записью пользователя, который входит в группу «Аудиторы» (User2).

21. Откройте командную строку.

22. Появится сообщение: Командная строка отключена администратором.

Задание 2. Установка единых обоев рабочего стола для всех пользователей домена

Настроить GPO, который устанавливает единые обои рабочего стола для всех пользователей в домене.

Реальный сценарий: В компании используется корпоративный стиль оформления рабочих столов с логотипом компании и едиными обоями для всех сотрудников.

1. Создайте папку для обоев на сервере: На диске C: создайте папку Public. Внутри папки Public создайте папку Wallpapers. Скопируйте файл изображения (например, wallpaper.jpg) в папку C:\Public\Wallpapers\.
2. Предоставьте доступ к папке:
3. Щелкните правой кнопкой мыши по папке C:\Public → «Свойства».
4. Перейдите на вкладку «Доступ» → «Общий доступ...».
5. Добавьте группу «Все» (Everyone) с правами «Чтение».
6. Нажмите «Поделиться» → «Готово».
7. Запишите сетевой путь к файлу. Например: Запишите сетевой путь к файлу. Например: SERVER01\Public\Wallpapers\wallpaper.jpg
8. В консоли «Управление групповой политикой» выберите контейнер: Лес: contoso.com → Домены → contoso.com → Объекты групповой политики
9. Щелкните правой кнопкой мыши контейнер «Объекты групповой политики» и выберите «Создать». В поле «Имя» введите: Единые обои рабочего стола. Нажмите ОК.

Настройка параметра политики

10. Щелкните правой кнопкой мыши GPO «Единые обои рабочего стола» и выберите «Изменить».
11. В редакторе GPO разверните путь: Конфигурация пользователя → Политики → Административные шаблоны → Рабочий стол
12. Дважды щелкните параметр «Обои рабочего стола».
13. Выберите вариант «Включено».
14. В поле «Имя обоев» введите полный сетевой путь к файлу: \\SERVER01\Public\Wallpapers\wallpaper.jpg
15. В поле «Стиль обоев» выберите один из вариантов:
16. **Растянуть** — изображение растягивается на весь экран (рекомендуется)
17. **Замостить** — изображение повторяется
18. **По центру** — изображение располагается по центру
19. **Заполнить** — изображение масштабируется с сохранением пропорций
20. Перейдите на вкладку «Комментарий» и введите: Устанавливает корпоративные обои рабочего стола для всех пользователей домена.
21. Путь к файлу: \\SERVER01\Public\Wallpapers\wallpaper.jpg
22. Нажмите **ОК**.
23. Закройте редактор GPO.

Настройка фильтров безопасности

24. В консоли «Управление групповой политикой» выберите GPO «Единые обои рабочего стола».
25. На вкладке «Область» (Scope) в секции «Фильтры безопасности»:
26. Убедитесь, что группа «**Authenticated Users**» присутствует (по умолчанию).
27. Это обеспечит применение политики ко всем пользователям домена.

28. **Важно:** Если оставить фильтр Authenticated Users, политика применится ко всем. Если нужно применить к конкретной группе — удалите Authenticated Users и добавьте нужную группу.

Шаг 5. Связывание GPO с доменом

29. В дереве консоли щелкните правой кнопкой мыши домен contoso.com.

30. Выберите «Связать существующий объект GPO».

31. В списке выберите «Единые обои рабочего стола».

32. Нажмите **ОК**.

Шаг 6. Применение политики на клиенте

33. На клиентском компьютере (CLIENT01) откройте командную строку от имени администратора.

34. Выполните команду: `cmd`

35. `gpupdate /force`

36. Выйдите из системы и войдите заново (обои применяются при входе пользователя).

Шаг 7. Проверка применения политики

Проверка 1. Визуальная проверка

37. Войдите на CLIENT01 под любым пользователем домена.

38. **Ожидаемый результат:** На рабочем столе отображается корпоративное изображение.

Проверка 2. Проверка через RSOP

39. Откройте оснастку «Результирующая политика»:

40. Win + R → введите `rsop.msc` → Enter.

41. В дереве оснастки перейдите к узлу: Конфигурация пользователя → Административные шаблоны → Рабочий стол

42. Найдите параметр «Обои рабочего стола» и убедитесь, что он имеет состояние «Включено» с правильным путем.

Часть 2: Делегирование и поддержка компьютеров

Многие предприятия содержат персонал для поддержки конечных пользователей — так называемый *отдел справки*. Сотрудники этого отдела устраняют неполадки, настраивают конфигурацию, а также выполняют задачи поддержки на клиентских компьютерах, для чего необходимы административные привилегии. Поэтому учетным записям персонала поддержки должен быть назначен уровень привилегий локальной группы Администраторы (Administrators) на клиентских компьютерах. Однако следует учесть, что уровень привилегий группы Администраторы домена (Domain Administrators) назначать не следует, поэтому

рекомендуется отконфигурировать клиентские системы, добавив членов команды отдела справки в локальную группу администраторов с помощью политики групп с ограниченным доступом. В этом задании мы рассмотрим принципы использования политики ограничения групп, с помощью которых можно добавить членов персонала поддержки в локальную группу Администраторы (Administrators) клиентов, делегировав таким образом команде справки задачу поддержки этих компьютеров. Эта же методика применяется для делегирования команде поддержки административных задач любых компьютеров.

Упражнение 6. Делегирование администрирования всех клиентов в домене

Создайте GPO с параметром политики групп с ограниченным доступом, который добавляет группу Справка в локальную группу Администраторы (Administrators) на всех клиентских компьютерах.

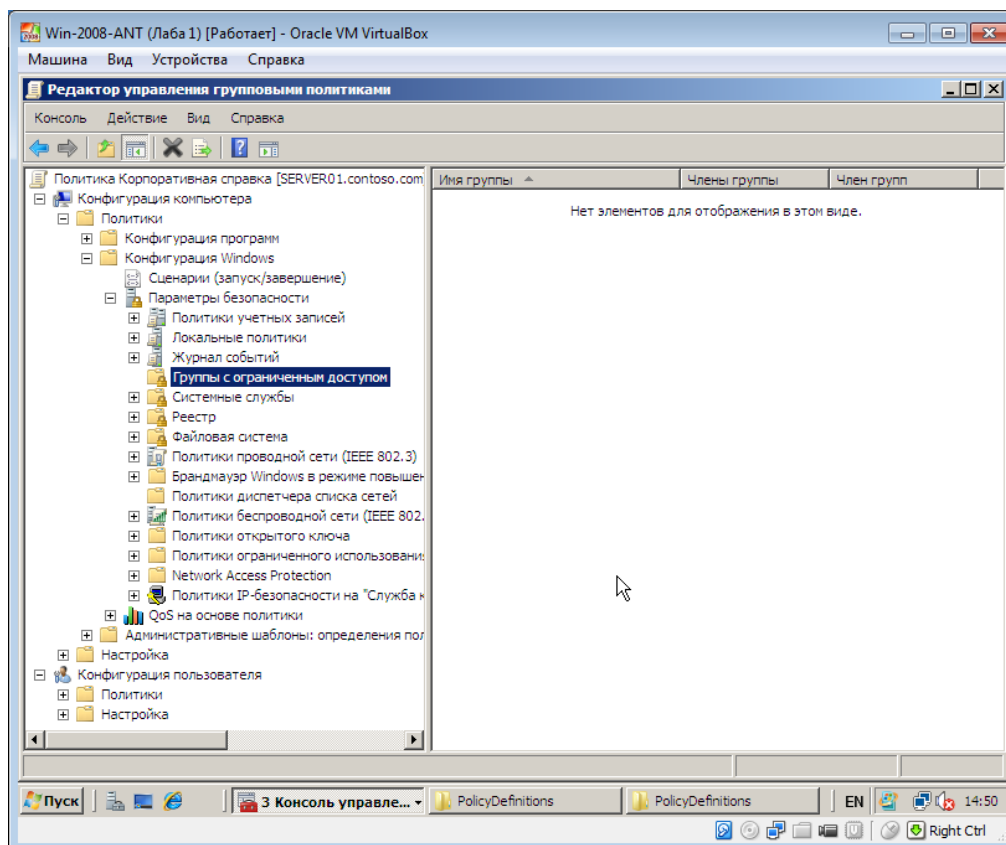
1. В консоли Управление групповой политикой (Group Policy Management) разверните узел Лес\Домены \contoso.com. Выберите контейнер Объекты групповой политики (Group Policy Objects).

2. Щелкните правой кнопкой мыши контейнер Объекты групповой политики и выполните команду Создать (New).

3. В поле Имя (Name) введите имя Корпоративная справка и щелкните ОК.

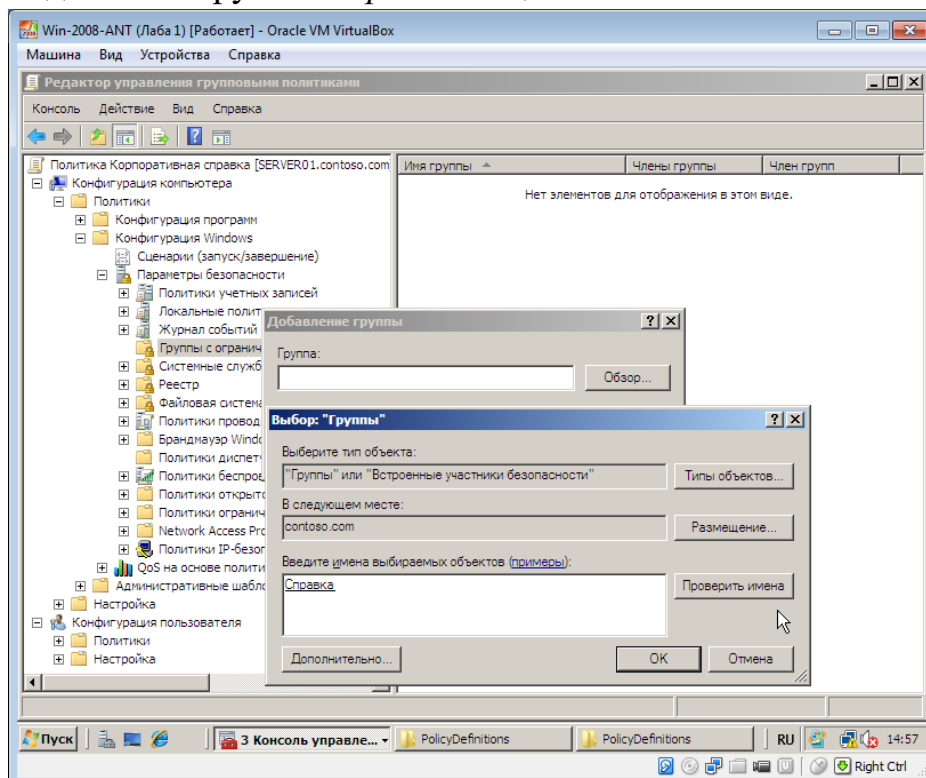
4. Щелкните правой кнопкой мыши созданный объект GPO и выполните команду Изменить (Edit). Параметры групповой политики

5. В редакторе управления групповыми политиками откройте узел Конфигурация компьютера \Политики\ Конфигурация Windows \Параметры безопасности \ группы с ограниченным доступом.



6. Щелкните правой кнопкой мыши узел Группы с ограниченным доступом выполните команду Добавить группу (Add Group).

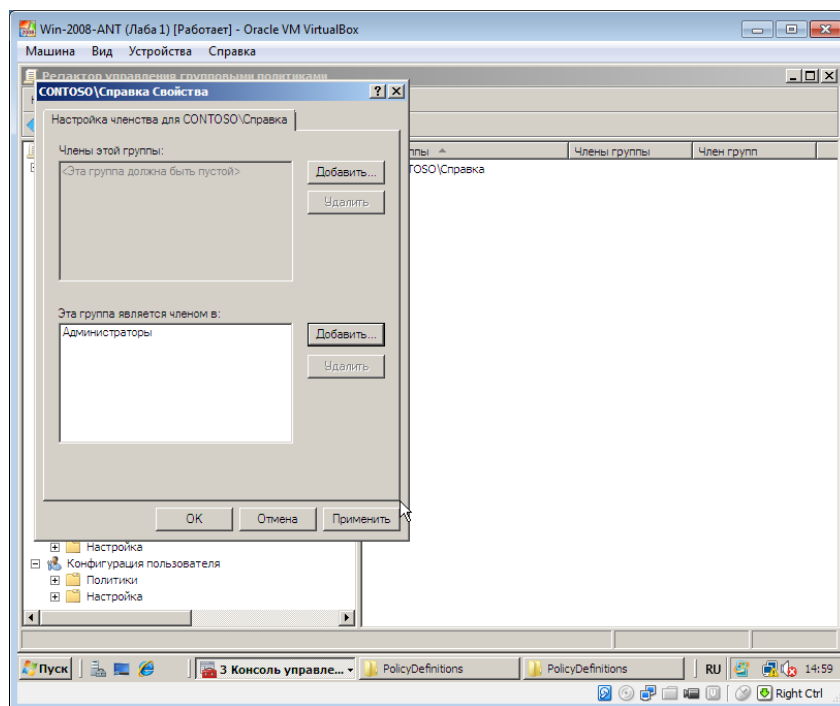
7. Щелкните кнопку Обзор (Browse), в диалоговом окне Выбор: "Группы" (Select Groups) введите имя группы *Справка* и щелкните ОК.



8. Закройте диалоговое окно Добавление группы (Add Group), щелкнув ОК.

9. Напротив секции Эта группа входит в щелкните кнопку Добавить (Add).

10. Введите имя группы Администраторы (Administrators) и щелкните ОК. Диалоговое окно свойств групповой политики должно выглядеть так, как показано на рисунке.



11. Вновь щелкните ОК, чтобы закрыть диалоговое окно Свойства (Properties).

12. Закройте редактор управления групповыми политиками.

13. В консоли Управление групповой политикой (Group Policy Management) щелкните правой кнопкой мыши подразделение Клиенты и выполните команду Связать существующий объект GPO (Link An Existing GPO).

14. Выберите объект групповой политики Корпоративная справка, щелкните ОК.

15. На клиентском компьютере (SERVER02) войдите под учетной записью пользователя, входящего в группу «Справка» (например, User1).

16. Попробуйте выполнить действие, требующее прав администратора: Откройте «Управление компьютером»: Щелкните правой кнопкой мыши по значку «Компьютер» на рабочем столе → «Управление».

- Если UAC (Контроль учетных записей) настроен по умолчанию, появится диалог подтверждения, но после нажатия «Да» действие будет выполнено.
- Окно «Управление компьютером» открывается без ошибок.