ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ

ВЫСШЕГО ОБРАЗОВАНИЯ

**БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ**

**ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ**

(НИУ «БелГУ»)

ИНСТИТУТ ИНЖЕНЕРНЫХ И ЦИФРОВЫХ ТЕХНОЛОГИЙ

КАФЕДРА МАТЕМАТИЧЕСКОГО

И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННЫХ СИСТЕМ

**Отчет по лабораторной работе 8**

**по дисциплине: «Компьютерные сети»**

студента очного отделения

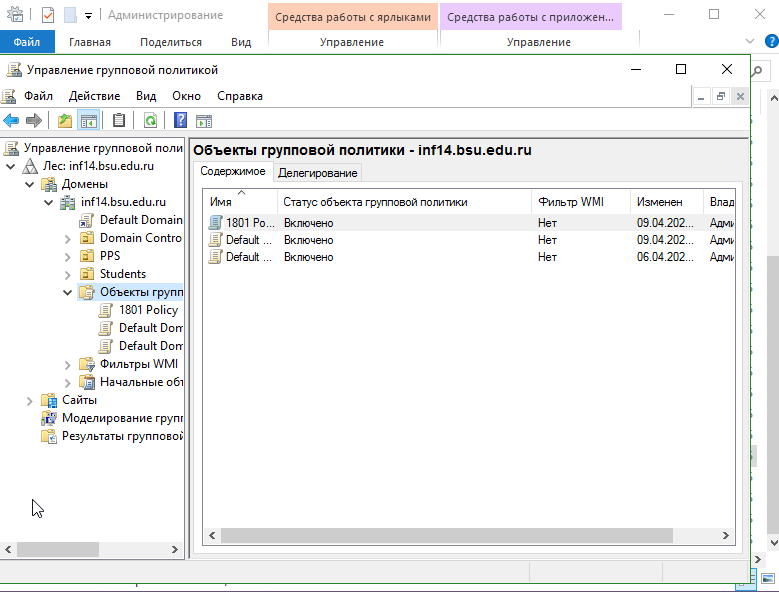
4 курса 12001801 группы

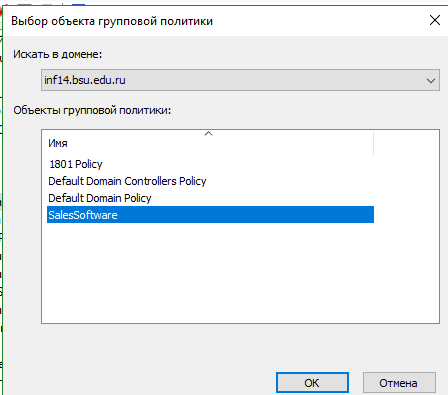
Капустина Виктора Сергеевича

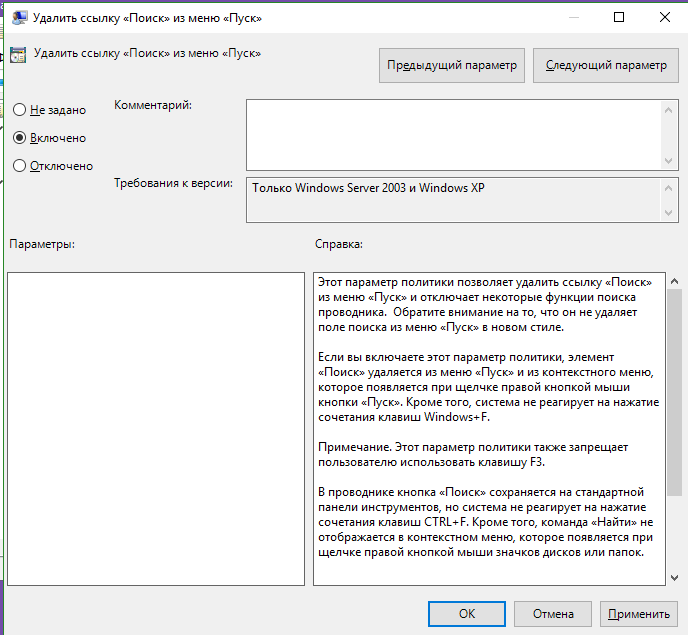
Проверил(а):

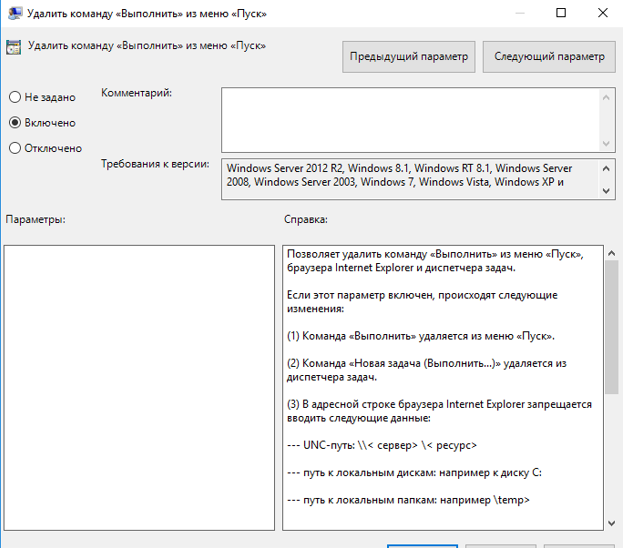
Маматов Евгений Михайлович

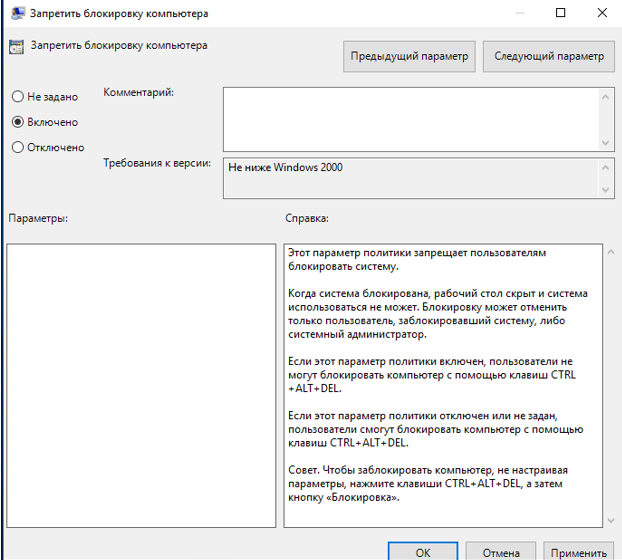
Белгород 2022

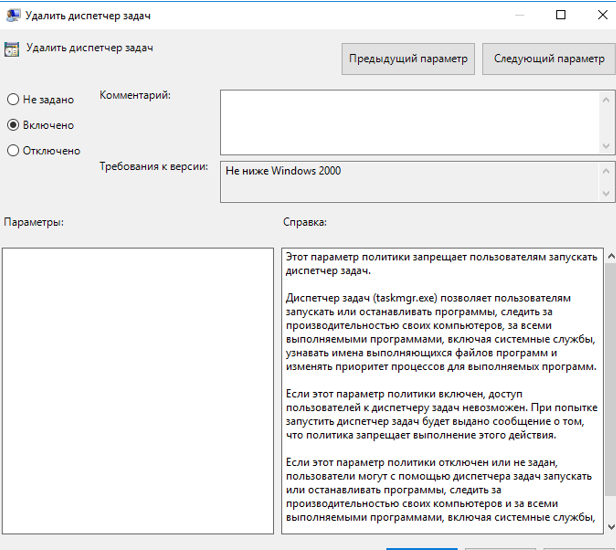
  
Рис. 1 Создание объекта групповой политики

  
Рис. 2 Связываем ОП sales и GPO SalesSoftware

  
Рис. 3 Изменение политики

  
Рис. 4 Изменение политики

  
Рис. 5 Изменение политики после нажатия Ctrl+Alt+Del

  
Рис. 6 Изменение политики на доступ к диспетчеру задач

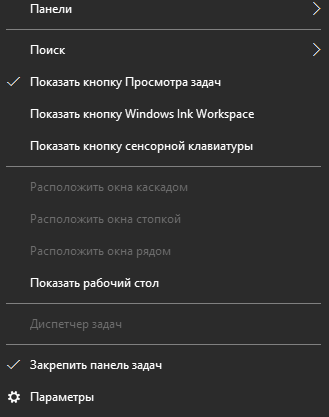


Рис. 7 Отсутствие разрешения для Диспетчера задач

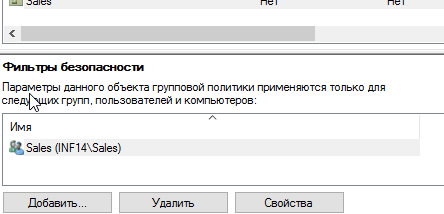


Рис.8 Добавление фильтра безопасности Sales

**1.** **Можно ли добавить к стандартным консолям Windows 2000 Server оснастки? Почему?**

Т.к. оснастки – это один из инструментов настройки оболочки Windows, то можно сделать вывод, что можно. Они используются для администрирования компьютера. Чтобы добавить оснастку нужно в меню «Пуск» выбрать команду «Выполнить» и ввести в командную строку mmc. Для подтверждения нажать OK. Появится окно управления. Открыть меню «Консоль» и использовать опцию «Добавить или удалить оснастку». Нажать «Добавить» и выбрать из списка нужную оснастку.

**2.** **Пользователи жалуются на окно, появляющееся каждый раз, когда они входят в систему. В меню Startup (Автозагрузка) нет ярлыков. После закрытия окна, выхода из системы и перезагрузки компьютера окно по-прежнему появляется при входе в систему. Какова наиболее вероятная причина этой проблемы и как ее устранить?**

Возможно у пользователя нет доступа к программе. Можно поменять настройки групповой политики. Также приложения могут быть настроены для автоматического запуска в качестве служб. Чтобы не дать работать приложению, настроенному для автоматического запуска в качестве службы, можно настроить его для запуска вручную. Могут быть назначены сценарии.

**3.** **В каких случаях использовать группы безопасности вместо групп распространения?**

Группы безопасности стоит использовать в том случае, если они будут использоваться для управления безопасностью (для назначения разрешений и предоставления доступа к ресурсам).

**4.** **Каковы последствия изменения режима домена со смешанного на основной?**

При изменении режима со смешанного на основной происходит следующее:

· прекращается поддержка репликации нижнего уровня

· запрещается добавление новых контроллеров нижнего уровня в данный домен;

· сервер, исполнявший роль основного контроллера домена, перестает быть таковым, поэтому все контроллеры становятся равноправными

**5.** **Что такое GPO, GPC и GPT?**

**Групповые политики** представляют собой набор параметров конфигурации, которые администратор групповой политики применяет к одному или нескольким объектам в хранилище Active Directory

## **GPO - Объекты групповой политики**

Содержат параметры узлов, доменов и ОП, которые записываются в хранилище Active Directory в *контейнер групповой политики* (group policy container, GPC). Кроме того, GP хранят данные групповой политики в структуре папок — *шаблоне групповой политик* (group policy template, GPT). Внутренняя структура GPO чаше всего скрыта от администратора.

Один или несколько объектов GPO могут быть применены к сайту, домену или ОП. Несколько контейнеров в хранилище Active Directory могут быть связаны с одним и те же

GPO, а один контейнер может иметь более одного GPO, связанного с ним. Облает действия GPO обусловлена членством в группах безопасности.

Небольшие и редко меняющиеся данные групповой политики хранятся в GPC.

Большие и часто меняющиеся данные групповой политики хранятся в GPT.

## **Локальные объекты групповой политики**

Существуют на каждом компьютере с Windows 2000, и по умолчанию в них сконфигурированы только параметры безопасности. Локальный GPO хранится в папке %systemroot%\System32\GroupPolicy и имеет следующие разрешения ACL:

ü Администраторы (Administrators) — Полный доступ (Full Control);

ü Система (SYSTEM) — Полный доступ (Full Control);

ü Прошедшие проверку (Authenticated Users) — Чтение и выполнение (Read & Execute), Список содержимого папки (List Folder Contents) и Чтение (Read). *Группы SYSTEM и Authenticated Users — системные.*

**GPC - Контейнеры групповой политики**

Это объекты Active Directory, хранящие свойства GPO и включающие подконтейнеры для компьютера и данных групповой политики пользователя. Сведения о версиях, содержащиеся в GPC, обеспечивают синхронизацию информации, хранящейся в GPC, с информацией GPT. GPC содержит также информацию о состоянии, указывающую, активен GPO или нет.

GPC содержит данные хранилища классов Windows для развертывания приложений. *Хранилище классов* (class store) — это основанное на сервере хранилище всех приложений, интерфейсов и API, обеспечивающих публикацию и назначение приложений.

**GPT -** Шаблон GPT Типы групповой политикиявляется структурой папки %systemroot%\SYSVOL\sysvol\<имя\_домена>\Policies на контроллерах доменов. GPT является контейнером, хранящим параметры политики для административных шаблонов, безопасности, ПО и сценариев.

## Структура GPT

При создании GPO создается и соответствующая структура папок GPT. Имя папки, присваиваемое GPO, является GUID созданного объекта GPO.

## Содержимое GPT

По умолчанию в GPT содержатся подкаталоги User и Machine и файл Gpt.ini. По мере создания и модификации политик создаются дополнительные папки. Структура папки зависит от настроенных Вами групповых политик.

**6.** **Преимущества групповой политики**

Групповые политики представляют собой набор параметров конфигурации, которые администратор групповой политики применяет к одному или нескольким объектам в хранилище Active Directory. С их помощью он управляет рабочей средой пользователей в домене и контролирует рабочую среду пользователей определенного ОП.

Задав соответствующие параметры групповой политики для определенных пользователей в сочетании с разрешениями NTFS, обязательными профилями и другими средствами безопасности Windows, можно предотвратить установку пользователями ПО и их доступ к запрещенным программам или данным. Можно также запретить пользователям удалять файлы, необходимые для правильного функционирования приложений или ОС.

Групповая политика позволяет защитить среду пользователя, настроив:

- автоматическое включение приложений в меню Start (Пуск) для пользователя;

- распространение приложений, чтобы пользователи легко находили их в сети и устанавливали;

- доставку файлов или ярлыков в нужные места сети или в папку на компьютере пользователя;

- автоматизацию выполнения заданий или программ в момент входа или выхода пользователя или в момент включения или выключения компьютера;

- переназначение папок на сетевые ресурсы для увеличения надежности хранения данных.

**7.** **Типы групповой политики**

| Тип групповой политики | Описание |
| --- | --- |
| Конфигурация программ | Указывает приложения, к которым пользователь может получить доступ. Этот тип позволяет автоматически устанавливать приложения:  **назначением приложения —** групповая политика автоматически устанавливает или обновляет приложения на клиентских компьютерах или обеспечивает пользователя связью с приложением, которое он не может удалить;  **публикацией приложения** — администратор групповой политики публикует приложения в Active Directory, затем они появляются в списке компонентов, которые пользователь может установить с помощью команды Add/Remove Programs в Control Panel;пользователь может удалить это приложение. |
| Сценарии | Позволяет администраторам групповой политики определять сценарии и командные файлы, выполняемые в определенное время, например при запуске или остановке системы или в момент входа или выхода пользователя. Сценарии автоматизируют повторяющиеся задания, такие как подключение сетевых дисков. |
| Службы удаленной установки (Remote Installation Services, RIS) | Управляет параметрами установки RIS, предлагаемыми мастером клиентской установки. |
| Параметры безопасности | Позволяет администраторам групповой политики ограничивать доступ пользователей к файлам и папкам, конфигурировать учетные ограничения (например, сколько раз пользователь может ввести неверный пароль, до того как Windows заблокирует его учетную запись), настраивать локальную политику (например, права и аудит пользователя), управлять сервисной работой служб, ограничивать доступ к реестру и журналу событий, настраивать доступ к открытому ключу и конфигурировать политику безопасности IP (IPSec). |
| Административные шаблоны | Включает групповые политики, позволяющие регулировать параметры реестра в отношении поведения и вида рабочего стола, включая компоненты ОС и приложения. |
| Перенаправление папок | Позволяет перенаправлять папки Windows с места, определенного профилем пользователя по умолчанию, на новое место в сети, где ими можно будет управлять централизованно. |

**8.** **Структура и объекты групповой политики**

Структура групповой политики

Групповые политики (group policies) — это наборы параметров конфигурации, применяемых к одному или нескольким объектам в хранилище Active Directory. Эти параметры находятся внутри объекта групповой политики (group policy object, GPO), который хранит данные групповой политики в контейнерах и шаблонах.

Объекты групповой политики

Содержат параметры узлов, доменов и ОП, которые записываются в хранилище Active Directory в контейнер групповой политики (group policy container, GPC). Кроме того, GP хранят данные групповой политики в структуре папок — шаблоне групповой политик (group policy template, GPT). Внутренняя структура GPO чаше всего скрыта от администратора.

Один или несколько объектов GPO могут быть применены к сайту, домену или ОП. Несколько контейнеров в хранилище Active Directory могут быть связаны с одним и те же GPO, а один контейнер может иметь более одного GPO, связанного с ним. Облает действия GPO обусловлена членством в группах безопасности.

Небольшие и редко меняющиеся данные групповой политики хранятся в GPC. Большие и часто меняющиеся данные групповой политики хранятся в GPT.

**9.** **Порядок наследования**

Как правило, групповая политика передается от родительского к дочернему контейнеру. Групповая политика, назначенная родительскому контейнеру верхнего уровня, применяется ко всем нижележащим контейнерам, включая расположенные в них объекты пользователя и компьютера. Однако групповая политика дочернего контейнера, параметры которой заданы явным образом, имеет более высокий приоритет, чем родительского контейнера.

Если параметры политики родительского ОП не сконфигурированы, дочернее ОП их не наследует. Опущенные параметры политики наследуются как неактивные. Аналогично, если для родительского ОП политика сконфигурирована, и та же самая политика не сконфигурирована для дочернего, последнее наследует политику родительского ОП.

Если родительская и дочерняя политики совместимы, дочернее ОП наследует политику родительского, и дочерняя настройка также применяется. Политики наследуются, пока они совместимы. Например, если родительская политика помещает определенную папку на рабочий стол, а для дочерних параметров нужна дополнительная папка, то пользователь видит обе папки.

Если политика родительского ОП конфликтует с политикой дочернего, политика первого не наследуется. Применяется настройка дочернего ОП.

**10.**  **Администрирование групповых политик**

***Управление настройками программ***

Для централизованного управления распространением ПО служит оснастка Group Policy. ПО может быть установлено, назначено, опубликовано, обновлено, исправлено и удалено для групп пользователей и компьютеров.

***Назначение и публикация приложений***

Можно назначать приложения пользователям и компьютерам и публиковать приложения пользователям.

***Назначение пользователям***

Пользователю, которому назначено приложение, предлагается установить его при следующем входе на рабочую станцию. Оповещение приложения следует за пользователем независимо от того, на каком компьютере он работает в настоящее время. Это приложение устанавливается, как только пользователь первый раз активизирует приложение на компьютере, выбрав его в меню Start (Пуск) или открыв связанный с ним документ.

***Назначение компьютерам***

Приложение, назначенное компьютеру, предлагается пользователям и устанавливается когда это безопасно — обычно при запуске компьютера, когда в нем нет конфликтующих процессов.

***Публикация пользователям***

Приложение, опубликованное пользователям, не появляется среди установленного на компьютерах ПО. Ни на рабочем столе, ни в меню Start ярлыков не видно, и в локальный реестр на компьютерах пользователей изменения не вносятся. Вместо этого опубликованные приложения хранят свои атрибуты оповещения в хранилище Active Directory. Затем информация, например имя приложения и файловые ассоциации, представляется пользователям в контейнере Active Directory.

***Управление сценариями***

Групповая политика Windows позволяет достаточно гибко назначить сценарии. Можно назначить компьютерам сценарии включения и выключения, а пользователям — сценарии входа и выхода, выполняемые в процессе регистрации пользователя в системе или выхода из нее.

***Управление параметрами безопасности***

Политика безопасности покрывает различные области политики, административных прав Разрешений пользователей. В Windows определены два вида политики безопасности:

1. домена;

2. компьютера (известна также как локальная политика).

На компьютер, не включенный в домен Windows, влияет только политика безопасности компьютера. К компьютеру – члену в домене Windows сначала применяется политика безопасности компьютера, а затем – политика безопасности домена. Windows предоставляет инфраструктуру для определения и централизованного управления этими политиками безопасности и соблюдает их на всех компьютерах в домене.