Лабораторная работа № 14

**Тема**:

«**Организация консоли администрирования** **Windows 7**»

**Цель работы**:практическое освоение инструмента управления операционнойсистемы Windows 7 – графической консоли администрирования ММС**.**

**Оборудование:** персональный компьютер(монитор,системный блок,клавиатура,мышь),ОС Windows, программа для виртуализации Oracle VM VirtualBox, образ виртуальной машины (Win7\_01).

1. **Теоретическая часть**

**Консоль управления Microsoft Management Console (MMC)** *группирует средства**администрирования, которые используются для администрирования сетей, компьютеров, служб и других системных компонентов.*

Консоль MMC непосредственно не выполняет административные функции, однако предоставляет возможности интеграции в нее компонентов или системных приложений, выполняющие эти функции. Основной тип интегрируемых на консоль компонентов называется оснасткой, которые не могут выполняться отдельно без консоли. Среди других добавляемых элементов могут быть элементы управления ActiveX, ссылки на Web-страницы, папки, видов панели задач и собственно задачи для выполнения. Дополнительные теоретические сведения об оснастках и других используемых для интеграции на консоль элементах будут добавлены в дальнейшем, в соответствующих разделах настоящей лабораторной работы.

Базовое окно консоли MMC представляет собой графическую форму с контекстными меню, реализующие дружественный пользовательский интерфейс. Имеется панель инструментов с командами создания, открытия и сохранения консолей и, кроме того, область описания и строка состояния в нижней части окна. Чтобы увидеть базовое окно, а также непосредственно саму консоль MMC, необходимо выполнить следующие действия:

* нажмите Пуск | Выполнить,
* наберите в появившемся окне MMC.exe (или просто mmc),
* нажмите Enter для ввода.

Новая консоль MMC представляет собой отдельное окно, разделенное на две вертикальные области, в левой из которых отображается дерево консоли с его корнем. Дерево консоли оказывает доступные элементы и компоненты консоли. Правая область является областью сведений, которая содержит описания элементов и выполняемых ими функций. Содержание области сведений соответствует выбранному элементу в дереве консоли и может включать Web-страницы, графики, диаграммы, таблицы и столбцы.

Создавая надежные средства управления компьютерами сети, можно собрать и настроить собственную консоль MMC, выполняющую заданные функции администрирования. После того как добавлены все необходимые элементы и компоненты консоли, панель главного меню, панель инструментов, а также область описания и строка состояния могут быть скрыты для предотвращения в дальнейшем нежелательных изменений. Созданные таким образом управляющие системы сохраняются в файлах с расширением .msc (Management Saved Console, сохраненная консоль управления) и могут быть, в частности, распространены в пределах всей системы посредством задания к ним доступа с помощью ярлыков или элементов меню Пуск.

Чтобы увидеть консоль управления локальным компьютером в качестве примера готовой и отлаженной консоли MMC, необходимо выполнить:

* нажмите Пуск | Выполнить,
* наберите в появившемся окне compmgmt.msc (или compmgmt),
* нажмите Enter для ввода.

Существует два основных режима доступа консоли администрирования, задающиеся непосредственно при ее создании:

* пользовательский, в котором можно администрировать систему, работая с уже существующими консолями,
* авторский, в котором можно создавать новые консоли или изменять существующие.

В свою очередь, имеется три уровня режима пользователя, что обусловливает всего четыре варианта предустановленного режима доступа:

* авторский режим;
* режим пользователя — полный доступ;
* режим пользователя — ограниченный доступ, многооконный;
* режим пользователя — ограниченный доступ, однооконный.

Консоль MMC, инициализированная в авторском режиме, предоставляет полный доступ ко всем ее возможностям, включая добавление и удаление оснасток, создание новых окон и панелей задач, а также просмотр любых частей дерева консоли и другие. Однако при выборе одного из трех режимов пользователя авторские возможности исключаются. В частности, если для консоли установлен параметр «пользовательский режим — полный доступ», то предоставляются все команды управления окном консоли и полный доступ к ее дереву, но запрещается добавление, удаление оснасток и изменение свойств консоли администрирования.

Изменения консоли MMC в авторском и пользовательском режимах сохраняются по-разному. При закрытии консоли в авторском режиме выводится диалоговое окно с предложением сохранить изменения. Однако в пользовательском режиме и снятом флажке «Не сохранять изменения для этой консоли» изменения будут сохранены автоматически при закрытии.

Если консоль открыта при соблюдении одного из следующих условий:

* в базовом окне при загрузке,
* с помощью команды контекстного меню Автор,
* в командной строке с параметром /a,

то предустановленный режим игнорируется, а открытие консоли осуществляется в авторском режиме.

Очевидно, что загрузка консоли MMC в авторском режиме не требуется рядовым пользователям. Системный администратор может настроить профили пользователей так, чтобы запретить им переход в авторский режим, как из командной строки, так и через контекстное меню. Кроме того, запрет перехода в авторский режим может быть организован при использовании возможностей групповой политики, при которой, в частности, осуществляется ограничение доступа к определенным оснасткам. Рассмотрению базовых возможностей оснастки групповой политики будет посвящена вторая часть настоящей лабораторной работы.

Прежде чем создавать новую консоль MMC, необходимо определить действия, для которых предназначена эта консоль, список администрируемых компонентов, оснасток и других элементов, которые потребуются для выполнения поставленных задач. Следует также рассмотреть необходимость создания видов панели задач. После принятия этих решений можно открыть новую консоль и начать добавлять элементы к дереву консоли. Полное руководство по созданию и настройке консолей MMC находится на Web-узле корпорации Майкрософт (http://www.microsoft.com).

В лабораторной работе предполагается ознакомление с основными принципами организации и построения консоли администрирования MMC, а также с базовыми возможностями основных инструментов системного администратора — оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).

Перед началом выполнения заданий в среде ОС Windows 7 необходимо выполнить следующее:

1. запустить виртуальную машину с ОС Windows 7 и активировать справочное меню (Пуск | Справка и поддержка);
2. ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;
3. ознакомиться возможностью получения сведений пункта 2 из альтернативного источника информации, доступного непосредственно в справке консоли администрирования MMC (Справка | Вызов справки);
4. ознакомиться с описанием и возможностями оснасток «Локальные пользователи и группы» и «Редактор объекта групповой политики» («Групповая политика»).
5. **Практическая часть**

**Задание 1. Изменение параметров и способов настройки консоли администрирования MMC**

Порядок выполнения:

I. Создание консоли администрирования MMC в авторском режиме требует выполнения следующих действий:

* нажмите Пуск | Выполнить,
* наберите в появившемся окне MMC.exe (или просто mmc),
* нажмите Enter для ввода.

Возможны следующие альтернативные варианты авторского запуска консоли администрирования:

A. запуск из командной строки, используя синтаксис:

**Mmc** *путь*\*имя*\_*файла*.**msc /a**,

где параметр:

*путь*\*имя*\_*файла*.**msc**—запускает консольMMCс одновременным открытием файласохраненной консоли с именем *имя*\_*файла*.**msc** (Приложение 2). Если файл консоли не указан, будет открыта новая консоль MMC.

/a — открывает консоль MMC в авторском режиме.

Дополнительными параметрами команды могут быть:

/64 — открывает 64-разрядную версию консоли MMC (MMC64). Этот параметр используется только при работе в ОС Windows 7 64-Bit Edition.

/32 — открывает 32-разрядную версию консоли MMC (MMC32). При работе в ОС Windows 7 64-Bit Edition в окне консоли MMC, запущенной с этим параметром, открываются 32-разрядные оснастки.

В. запуск из файлового менеджера Проводник ОС Windows 7:

* наведите манипулятор мышь на файл с расширением .msc, находящийся в системной папке ОС (%systemroot%\system32\),
* кликните правой кнопкой мыши на файле и из контекстного меню выберите Автор.

1. Настройка параметров консоли администрирования MMC предназначена для ее конфигурирования с целью придания ей уникального вида.

**Содержание задания**

Для придания уникального вида сохраненной (новой) консоли администрирования MMC в авторском режиме выполните следующие действия:

1. В меню Консоль выберите команду Параметры.
2. На вкладке Консоль в поле названия введите новый заголовок.
3. На вкладке Консоль выполните следующие действия:

* нажмите кнопку Сменить значок,
* в поле Имя файла введите путь к файлу, содержащему значки (например,

%systemroot%\system32\shell32.dll),

* в поле Текущий значок выберите необходимый значок,
* кликните OK для ввода и Применить для подтверждения.

1. На вкладке Консоль из списка Режим консоли выберите пользовательский режим с полным доступом, в котором будет открываться консоль MMC при ее непосредственном запуске,
2. Для установленного в предыдущем пункте режима выполните указанные ниже действия:

* запретите изменение консоли MMC при ее непосредственном запуске, установив флажок «Не сохранять изменения для этой консоли», сделайте активным диалоговое окно Вид | Настройка вида консоли MMC при запуске, установив флажок «Позволить пользователю настраивать вид консоли»,

1. Если необходимо удалить файлы, содержащие параметры отображения файлов консоли, на вкладке Очистка диска нажмите кнопку Удалить файлы.
2. Сохраните окончательно сконфигурированную консоль администрирования MMC, выбрав самостоятельно ее имя и путь к месту расположения в меню Консоль | Сохранить как… При сохранении обратите внимание на то, что файлы консоли по умолчанию

размещаются в папке «Администрирование», имеющей полный путь %Pathname%\Главное меню\Программы\Админи-стрирование\.

1. Закройте сконфигурированную и сохраненную консоль администрирования MMC, выполнив соответствующие необходимые действия.

В файловом менеджере Проводник ОС Windows 7 выполните следующие инструкции:

* наведите манипулятором мышь на сохраненный файл консоли администрирования MMC и, дважды кликнув на нем, запустите консоль,
* откройте диалоговое окно Вид | Настройка вида и, изменяя положение флажков, обратите внимание на получаемый результат,
* изменив вид консоли MMC приемлемым образом, кликните OK для подтверждения полученного результата,
* в контекстном меню Консоль кликните Выход,
* снова запустите консоль администрирования MMC, кликнув манипулятором мышь на сохраненном файле консоли,
* изучите полученный результат,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 2. Добавление различных элементов и компонентов к дереву консоли администрирования MMC**

Основным, интегрируемым на консоль компонентом является оснастка. Оснастки существуют двух видов:

* изолированные,
* расширения.

Изолированная оснастка (или просто оснастка) добавляется к дереву консоли MMC без предварительного добавления других элементов, то есть непосредственно в корень дерева консоли.

Оснастка расширения (или просто расширение) всегда добавляется к другой изолированной оснастке или расширению, которые уже имеются в дереве консоли MMC. Если для определенной оснастки разрешены расширения, то, как правило, они работают с объектами, управляемыми непосредственно этой оснасткой, например, с компьютером, принтером, модемом или другим внешним устройством.

* дереве консоли оснастки и расширения располагаются для удобства иерархически или по группам. При добавлении новой оснастки или расширения, они появляются в виде нового элемента в дереве консоли MMC или в виде нового пункта контекстного меню, дополнительной панели инструментов, страницы свойств, а также возможно мастера, организующего определенную последовательность действий, к уже установленной оснастке.

Другими элементами, по необходимости применимыми для интеграции на консоль администрирования MMC, являются виды панели задач и собственно задачи, которые могут включать в себя команды меню для элементов консоли и команды, запускаемые из командной строки. Кроме того, могут быть созданы команды, действующие как часть дерева консоли или открывающие другой компонент.

Прежде всего, перед добавлением указанных элементов к консоли MMC, необходимо определить их число. Если, в частности, требуется добавить несколько видов панели задач, то наряду с этим необходимо определить тип каждой панели (для отображения списка и задач или только задач), а также разделить задачи по интегрированным видам панели. Добавление видов панели задач и собственно задач осуществляется посредством работы мастера создания этих элементов. При этом важно помнить, что консоль MMC должна содержать, по крайней мере, одну оснастку, чтобы возможность интеграции появилась в принципе.

Отдельной возможностью, иногда необходимой при администрировании сетей, является добавление элементов и компонентов дерева консоли администрирования MMC в виде списка ярлыков в меню «Избранное».

Дополнительные сведения о добавлении различных элементов в дерево консоли администрирования MMC можно получить, воспользовавшись справкой ОС Windows 7 (Пуск | Справка и поддержка) в разделе Общее представление о MMC \ Консоль MMC в авторском режиме \ Оснастки \ Создание консолей.

**Содержание задания**

Первым необходимым компонентом, добавляемым к дереву консоли администрирования MMC при ее организации и построении, является оснастка. Для добавления оснастки в авторском режиме выполните следующие действия:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. В меню Консоль выберите команду Добавить или удалить оснастку.
3. В диалоговом окне Добавить/удалить оснастку нажмите кнопку Добавить вкладки Изолированная оснастка. Список Оснастки в диалоговом окне Добавить/удалить оснастку определяет элемент дерева консоли, к которому выполняется добавление элементов. В этом списке можно найти любой элемент дерева консоли. Обратите внимание на то, что по умолчанию это Корень консоли.
4. В диалоговом окне Добавить изолированную оснастку, выберите оснастки Службы из списка доступных в системе, кликнув на ней манипулятором мышь и нажав кнопку Добавить. Для добавления другой оснастки из списка, повторите указанные действия настоящего пункта повторно.
5. Для некоторых оснасток в процессе их инсталляции выводится диалоговое окно Выбор целевого компьютера, определяющее чем, устанавливаемая оснастка, будет управлять в дальнейшем — локальным или сетевым компьютером. Выберите Локальный компьютер, установив переключатель в соответствующее положение.
6. Нажмите Готово, Закрыть и затем кликните OK для подтверждения ввода.
7. Скройте меню и панель инструментов оснастки Службы, выполнив действия указанные ниже:

* В меню Вид выберите команду Настроить,
* В группе Оснастка снимите флажок Меню,
* В группе Оснастка снимите флажок Панели инструментов.

При устанавливании или снятии флажков, соответствующие им меню и панели инструментов отображаются или скрываются, причем, для всех оснасток консоли, включая текущую. Если переключение флажков не приводит к изменению вида консоли, тогда текущая оснастка не имеет специальных меню или панелей инструментов.

1. Не закрывая консоль администрирования MMC, сохраните ее, выбрав команду Сохранить в меню Консоль.

Для добавления расширений к уже установленной в предыдущем задании оснастке Службы выполните следующее:

1. В меню Консоль выберите команду Добавить или удалить оснастку.
2. В диалоговом окне Добавить/удалить оснастку выберите вкладку Расширение. На этой вкладке можно выбрать любой элемент дерева консоли из списка Оснастки, которые могут быть расширены, и просмотреть Доступные расширения, которые могут быть включены или отключены. После подключения расширение автоматически размещается в дереве консоли под оснасткой, к которой оно относится. Если дерево консоли содержит больше одного экземпляра оснастки, к которой подключено расширение, все остальные экземпляры автоматически получают это расширение. Среди Доступных расширений оснастки Службы удалите флажок с расширения Расширенный вид и отметьте к чему привело это действие. Повторите аналогичные действия с другими расширениями данной оснастки и изучите получаемый результат.
3. Не закрывая консоль администрирования MMC, сохраните ее. В окне консоли администрирования выполните следующие инструкции:

* последовательно перебирая доступные в системе оснастки, найдите те из них, которые обладают дополнительным меню, панелью инструментов или расширениями,
* изучите полученный результат и сделайте вывод о проделанной работе,
* запишите полученную информацию в отчет, заполнив табл. 13. Таблица 13. Результат поиска оснастки

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № |  | **Результат поиска** | **и вывод по** | **способу применения** |  |
| **Оснастка** | **дополнительных** | **меню, панелей** | **инструментов и/или** |  |
| п.п. |  |
|  | **расширений оснасток** | |  |  |
|  |  |  |  |
|  |  |  |  |  |  |
| 1 |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
| n |  |  |  |  |  |
|  |  |  |  |  |  |

**Задание3. Создание нового вида панели задач консоли администрирования MMC**

**Содержание задания**

Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. Добавьте оснастку Службы в корень консоли MMC.
3. В дереве консоли кликните манипулятором мышь на этой оснастке.
4. В меню Действие или кликнув правой кнопкой манипулятора на оснастке, выберите команду Новый вид панели задач.
5. Следуйте инструкциям «Мастера создания вида панели задач», чтобы добавить на консоль новую панель вида.
6. Если сразу после создания вида панели задач необходимо создать задачи, установите флажок «Запустить мастер создания новой задачи» на последнем экране «Мастера создания вида панели задач».
7. Следуйте инструкциям «Мастера создания новой задачи», чтобы добавить
8. на консоль новую задачу к существующей панели вида. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), связанный с видом панели задач, затем в меню Действие выберите команду Правка вида панели задач.
9. На вкладке Задачи нажмите кнопку Создать.
10. Повторите инструкции пункта 7 настоящего задания.
11. Не закрывая консоль администрирования MMC, сохраните ее.

Измените вид панели задач сохраненной консоли администрирования MMC, выполнив следующие действия:

* введите новое имя,
* введите новое описание,
* установите переключатель Стиль для области сведений в положение, соответствующее новому формату списка,
* удалите соответствующий флажок, чтобы скрыть стандартную вкладку,
* установите переключатель Стиль для описания задачи в положение, соответствующее новому стилю задачи,
* выберите новое значение ширины для вертикального списка или высоты для горизонтального списка,
* нажмите кнопку Параметры и установите переключатель в одно из необходимых положений,
* нажмите OK для подтверждения ввода,
* изучите полученный результат,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 4. Добавление элементов и компонентов дерева консоли в виде списка ярлыков в меню «Избранное»**

**Содержание задания**

Для добавления элемента или компонента в авторском режиме выполните следующее:

1. Создайте новую Консоль управления MMC одним их описанных в пункте I текущего учебного задания способов.
2. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), который нужно добавить в список «Избранное».
3. В области сведений выберите вкладку вида панели задач, которую нужно добавить, в случае, если для элемента или компонента, указанного в дереве консоли, настроен вид панели задач. В противном случае в области сведений вкладки не видны.
4. Выберите в меню Избранное команду Добавить в избранное.

* В поле Создать в диалогового окна Добавление в папку «Избранное» выполните указанные ниже действия: создайте новую папку с названием, выбранным самостоятельно, кликнув папку, которая будет выступать в качестве родительской для создаваемой папки и нажав кнопку Создать папку,
* нажмите кнопку OK для ввода,
* в поле Имя папки введите имя, под которым будет добавлен элемент,
* кликните OK для подтверждения ввода.

1. Не закрывая консоль администрирования MMC, сохраните ее. Упорядочите «Избранное» сохраненной консоли администрирования MMC, выполнив следующие действия:

* добавьте новую папку, введя ее имя в соответствующее поле и кликнув OK для подтверждения ввода,
* переместите элемент, созданный в пункте 5 настоящего задания, в новую, только что созданную, папку и кликните OK для ввода,
* переименуйте выбранный элемент и нажмите клавишу Enter для подтверждения ввода,
* удалите все элементы, расположенные ниже папки «Избранное»,
* нажмите Закрыть для завершения задания,
* изучите полученный результат,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 5. Ознакомление с оснасткой «Локальные пользователи и группы»**

Порядок выполнения:

Первым шагом при создании пользовательской консоли администрирования является придание ей функций контроля и управления учетными записями пользователей и групп. В среде ОС Windows 7 учетные записи локальных пользователей и групп управляются одноименной оснасткой «Локальные пользователи и группы».

Учетная запись пользователя содержит все сведения, определяющие пользователя. К этим сведениям относятся имя пользователя и пароль, требуемые для входа в систему, имена групп, членом которых он является, а также права и разрешения, которые он имеет при работе и доступе к системным ресурсам системы.

Существует два основных типа учетных записей пользователей, доступных на компьютере с ОС Windows 7: учетная запись администратора и учетная запись с ограниченными правами. Кроме того, штатная учетная запись гостя доступна для пользователей, не имеющих собственных учетных записей в системе. Учетная запись администратора предназначена для тех уполномоченных пользователей, кто может вносить изменения на уровне системы, устанавливать приложения и иметь полный доступ ко всем файлам и другим учетным записям. Она позволяет:

* создавать, изменять и удалять любые учетные записи,
* создавать и изменять имена и пароли пользователей,
* обеспечить наличие, по крайней мере, одного пользователя с учетной записью администратора, когда уже нет других учетных записей с подобными правами.

Учетная запись с ограниченными правами предназначена для пользователей, которым запрещается изменять большинство настроек системы, а также удалять важные файлы. Пользователь с такой учетной записью:

* не может устанавливать приложения и оборудование, но имеет доступ к уже существующим программам в системе,
* не может изменять имя и тип собственной учетной записи,
* может создавать, изменять или удалять собственный пароль,
* может изменять рисунок, назначенный учетной записи.

Необходимо помнить, что некоторые приложения могут работать некорректно для пользователей с ограниченными правами. В этом случае следует сменить тип учетной записи на администратора.

Учетная запись гостя предназначена для пользователей, не имеющих собственных учетных записей в системе. У записи гостя нет пароля, что позволяет быстро входить в систему, в частности, для проверки электронной почты или просмотра Интернета. Пользователь с учетной записью гостя:

* не может устанавливать приложения и оборудование, но имеет доступ к уже существующим программам в системе,
* не может изменить собственной тип учетной записи,
* может изменять рисунок, назначенный учетной записи.

Совокупность пользователей, компьютеров и контактов называется группой. Существуют группы безопасности, которые используются для управления доступом или в качестве списков рассылки и группы распространения, применяемые только в электронной почте.

Набор учетных записей пользователей представляет собой учетную запись группы. При включении учетной записи пользователя в определенную группу соответствующий пользователь получает все права и разрешения, предоставленные этой группе. **Содержание задания**

1. Создайте пользовательскую консоль администрирования одним из изученных в предыдущем учебном задании способов и сконфигурируйте ее должным образом, приняв во внимание ее целевую принадлежность.
2. Добавьте оснастку «Локальные пользователи и группы» в корень консоли администрирования.
3. Создайте две учетные записи для двух разных пользователей. Имена, описание и пароли выберите самостоятельно.
4. Установите флажки «Потребовать смену пароля при следующем входе в систему» для первого пользователя и «Запретить смену пароля пользователем» для второго.
5. Создайте локальную группу, имя и описание которой выберите самостоятельно.
6. Поместите в новую локальную группу созданных ранее пользователей, воспользовавшись диалоговым окном Свойства каждого из них.
7. Поместите в новую локальную группу пользователя Администратор, воспользовавшись диалоговым окном Свойства этой группы (см. пункт 5 секции). Обратите внимание на то, что в этой локальной группе уже присутствуют учетные записи двух созданных ранее пользователей.
8. Выбрав самостоятельно имя и путь к месту расположения, сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

* перенесите последовательность выполняемых действий по каждому из пунктов 1-8 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
* дважды войдите в систему под именами пользователей, соответствующих созданным учетным записям,
* обратите внимание на то, каким образом осуществляется влияние установленных в пункте 4 флажков на работу компьютера при смене пользователя,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 6. Взаимосвязь утилиты «Учетные записи пользователей» с оснасткой «Локальные пользователи и группы» при смене типа учетной записи**

**Содержание задания**

1. В Панели управления загрузите утилиту «Учетные записи пользователей», позволяющую изменять параметры и пароли учетных записей пользователей непосредственно в ОС

Windows 7.

1. Загрузите пользовательскую консоль администрирования, созданную в Секции А текущего задания, с возможностью ее редактирования.
2. Создайте новую ограниченную учетную запись, воспользовавшись утилитой «Учетные записи пользователей».
3. Перейдите в оснастку «Локальные пользователи и группы» загруженной консоли администрирования и отметьте, в какую из локальных групп была по умолчанию определена вновь созданная учетная запись.
4. В окне утилиты «Учетные записи пользователей» измените тип данной учетной записи с ограниченного на административный.
5. Снова перейдите в оснастку «Локальные пользователи и группы» загруженной консоли администрирования и убедитесь в том, что смена типа учетной записи привела к перемещению пользователя из группы Пользователи в Администраторы, тем самым, расширяя его права.
6. Удалите этого пользователя из групп Пользователи и Администраторы.
7. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий используйте следующие инструкции:

* перенесите последовательность выполняемых действий по каждому из пунктов 1-8 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
* обратите внимание на то, каким образом осуществляется взаимосвязь утилиты «Учетные записи пользователей» с оснасткой «Локальные пользователи и группы» при смене типа учетной записи,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 7. Возможности оснастки «Локальные пользователи и группы» при работе с профилями пользователей**

Профиль пользователя определяет параметры конфигурации рабочей среды, например, индивидуальную настройку экрана, сетевых подключений и доступа к принтеру. Эти параметры могут быть заданы самим пользователем или системным администратором. Существуют следующие виды профилей пользователя:

* локальный профиль, представляющий собой машинную запись об авторизованном пользователе, автоматически создаваемую на компьютере при первом входе на рабочую станцию или сервер, и 7анящийся на локальном жестком диске. Любые изменения локального профиля действительны только в рамках компьютера, на котором они произведены.
* перемещаемый профиль это находящийся на сервере профиль пользователя, который загружается на локальный компьютер при входе в систему и обновляется на локальном компьютере и сервере при выходе из нее. Если локальная копия профиля является более новой, чем копия на сервере, то пользователь имеет возможность использовать ее при очередном входе в систему.
* обязательный профиль это перемещаемый профиль, в котором можно задать конкретные параметры для отдельных пользователей или их группы. Этот профиль загружается всякий раз, когда осуществляется вход в систему и не обновляется при выходе из нее. Он может быть изменен только членом группы Администратор.

**Содержание задания**

1. Загрузите пользовательскую консоль администрирования, созданную в Секциях А и B текущего задания, с возможностью ее редактирования.
2. На локальном диске D: создайте папку, выбрав ее имя самостоятельно, для 7анения в ней профилей пользователей. Эта папка верхнего уровня, которая будет содержать индивидуальные папки профилей пользователей.
3. Создайте вложенную внутрь папку, предназначенную для непосредственного 7анения профиля пользователя.
4. Скопируйте профиль Администратора в созданную в пункте 3 секции папку, воспользовавшись системными средствами ОС Windows 7 в окне свойств системы (Панель управления | Система). При этом в диалоговом окне Копирование профиля разрешите использование для Всех пользователей.
5. В существующую консоль добавьте локальную оснастку «Общие папки». В доступных командах вложенной директории «Общие ресурсы» оснастки кликните Новый общий ресурс…и, следуя инструкциям Мастера создания общей папки, откройте Всем пользователям полный доступ для директорий, созданных в пунктах 2 и 3 секции. При этом новый общий ресурс должен появиться в столбце «Общая папка» в области сведений консоли администрирования. На вкладке Безопасность диалогового окна Свойства новых общих ресурсов нажмите кнопку Дополнительно и во вновь появившемся диалоговом окне установите флажок Наследовать от родительского объекта…
6. В виде профиля пользователя подключите только что скопированный в нестандартную папку профиль Администратора к одному из ранее созданных в Секции А пользователей, воспользовавшись его диалоговым окном Свойства.
7. В виде домашней папки подключите сетевой диск «H» на нестандартную папку с профилем Администратора к другому из ранее созданных в Секции А пользователей, воспользовавшись его диалоговым окном Свойства.
8. Создайте Новый вид панели задач таким образом, чтобы имелась возможность добавлять нового пользователя или группу, а изменять, удалять или переименовывать их возможности не было.
9. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

* перенесите последовательность выполняемых действий по каждому из пунктов 1-9 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
* дважды войдите в систему под именами пользователей, соответствующих созданным учетным записям,
* проверьте результат подключения профилей в пунктах 6 и 7 секции: нажмите Пуск | Выполнить, наберите в появившемся окне SendTo и нажмите Enter для ввода, в строке Адрес: появившегося окна отметьте полный путь папки SendTo, удостоверяющий правильную загрузку подключенного профиля.
* обратите внимание на то, каким образом осуществляется влияние подключенных в профилей на работу компьютера при смене пользователя,
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 8. Основные возможности оснастки «Редактор объекта групповой политики»**

Административное средство Active Directory предназначено для решения повседневных задач сетевого управления, в число которых входят: создание, удаление, изменение, перемещение

* предоставление разрешений на объекты каталога. Объектами управления могут являться подразделения, пользователи, контакты, группы, компьютеры, принтеры, а также объекты общих файлов.

Active Directory обеспечивает системного администратора иерархическим представлением сети и едиными возможностями управления всеми сетевыми объектами ОС Windows 2000 Server, где она является основой групповой политики. Для реализации указанных возможностей в ОС Windows 2000 Server имеются три оснастки «Пользователи и компьютеры Active Directory», «Домены и доверие Active Directory» и «Сайты и службы Active Directory», первые две из которых предназначены для создания объектов групповой политики домена или подразделения, третья — соответственно, для создания объекта групповой политики сайта. Для запуска этих оснасток из ОС Windows 7 необходимо осуществить подключение к удаленному столу сервера с установленными средствами администрирования ОС Windows 2000 Server, поскольку служба каталогов Active Directory в ОС Windows 7 является по умолчанию не доступной.

Понятие групповая политика в области администрирования применяется не только к пользователям и компьютерам, но и к серверам, контроллерам доменов и другим компьютерам под управлением ОС Windows 7. По умолчанию групповая политика применяется к домену и влияет на все его компьютеры и пользователи. Обеспечение групповой политики подразумевает конфигурирование системы и задания набора условий и параметров групповой политики, приводящих к определенным ограничениям или разрешениям в ОС.

Параметры групповой политики определяют различные компоненты конфигурации пользователя, в частности, окружения пользовательского рабочего стола (программы, доступные пользователям, программы, отображающиеся на рабочем столе, и параметры меню Пуск) и конфигурации компьютера, включая параметры, применяемые вне зависимости от того, кто работает на этих компьютерах. Чтобы создать частную конфигурацию компьютера для определенной группы пользователей используется оснастка «Редактор объекта групповой политики».

Набор указанных параметров групповой политики содержится в объекте групповой политики, который, в свою очередь, связан с выбранными объектами Active Directory — сайтами, доменами или подразделениями. Объектами групповой политики являются документы, создаваемые оснасткой. Они 7анятся на уровне домена и оказывают влияние на пользователей и компьютеры доменов и подразделений. Кроме того, каждый компьютер с ОС Windows 7 имеет единственную, 7анящуюся локально, группу параметров, которая называется локальным объектом групповой политики.

Все многообразие параметров групповой политики содержится в соответствующих расширениях оснастки «Групповая политика», посредством которых системному администратору предоставляются широкие возможности по управлению процессами и ресурсами ОС Windows 7:

* на основе реестра, используя расширение Административные шаблоны (A). При этом создается файл, содержащий параметры реестра, записанные в область базы данных реестра пользователя, в разделе HKEY\_CURRENT\_USER и в разделе HKEY\_LOCAL\_MACHINE для локального компьютера.
* посредством расширения Назначение сценариев (B). Групповая политика указывает сценарии входа/выхода пользователей из системы и загрузки/завершения работы.
* используя Редактор перенаправления папок (C). Групповая политика имеет возможность перенаправить системные папки «Мои документы» и «Мои рисунки», из папки «Documents and Settings» локального компьютера в новое место расположения в сети.
* на основе расширения Установка программ (D), которое позволяет назначать, публиковать и восстанавливать приложения.
* посредством расширения Параметры безопасности (E), позволяющей устанавливать ограничения на использование программ, политику отрытого ключа, а также осуществлять управление политикой безопасности IP.

Административные шаблоны это текстовые файлы с расширением .adm, содержащие сведения о политике для элементов, расположенных в папке «Административные шаблоны» оснастки. В ОС Windows 7 доступно четыре файла административных шаблонов, приведенных в табл. 14.

Файлы административные шаблонов состоят из иерархии категорий и подкатегорий, которые вместе определяют отображение параметров групповой политики. В них содержатся следующие сведения:  размещение параметров реестра, соответствующих каждому параметру административного шаблона групповой политики,

 величина параметров или ограничений, связанных с каждым параметром административного шаблона,

* значение по умолчанию для большинства параметров,
* объяснение функции каждого параметра,
* версии ОС Windows, поддерживающие каждый параметр.

**Таблица 14**.Административные шаблоны ОСWindows7

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Шаблон | **Справка по параметрам** | **Описание** |  |  |  |  |
| (.adm) |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | |  |  |  |
| System | %systemroot%\help\system.chm | В групповой | | политике | шаблон |  |
|  |  | установлен | по | умолчанию для | |  |
|  |  | клиентов ОС Windows 2000 и 7 | | | |  |
|  |  |  | | | |  |
| Inetres | %systemroot%\ help\inetres.chm | В групповой политике шаблон Internet | | | |  |
|  |  | E7lorer установлен по умолчанию для | | | |  |
|  |  | клиентов ОС Windows 2000 и 7 | | | |  |
|  |  |  | | | |  |
| Wmplayer | %systemroot%\help\wmplay.chm | Параметры WMP для клиентов ОС | | | |  |
|  |  | Windows 2000 и 7 | |  |  |  |
|  |  |  |  | |  |  |
| Conf | %systemroot%\help\conf1.chm | Параметры | программы | | NetMeeting |  |
|  |  | для клиентов ОС Windows 2000 и 7 | | | |  |
|  |  |  |  |  |  |  |

В среде ОС Windows 7 имеется возможность использования сценариев посредством двух серверов Wscript.exe или Cscript.exe, поддерживающих как Visual Basic Scripting Edition (расширение .vbs), так и JScript (расширение .js) файлы. В частности, в средствах оснастки «Групповая политика» имеется два расширения, расположенные в узлах консоли «Конфигурация компьютера | Конфигурация Windows» или «Конфигурация пользователя | Конфигурация Windows», позволяющие развертывать сценарии с использованием указанных серверов ОС Windows 7. Эти расширения следующие:

* сценарии (запуск/завершение) — расширение, посредством которого можно указать локально выполняемый сценарий при запуске и завершении работы компьютера.
* сценарии (вход/выход из системы) — расширение, посредством которого можно указать выполняемый сценарий при входе и выходе пользователя из системы. Эти сценарии запускаются с правами пользователя, а не администратора.

Перенаправление папки используется для перемещения некоторых специальных папок, например «Мои документы» и «Мои рисунки», в заданное место в сети, для их последующего доступа с разных узлов. В ОС Windows 7 возможны следующие специальные папки для перенаправления (табл. 15).

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Таблица 15.** Специальные папки ОСWindows7 | |  |  |  |
|  |  |  |  |  |
| Специальная | **Примечания** |  |  |  |
| папка |  |  |  |
|  |  |  |  |
|  |  | | |  |
|  | Параметры групповой политики управляют поведением папки «Application | | |  |
|  | Data» при включении кэширования на стороне клиента. Параметры | | |  |
|  | расположенывдеревеконсоли«Групповаяполитика»в | | |  |
| Application Data | Административных шаблонах\Сеть\Автономные файлы. | |  |  |
|  |  |  |  |
|  |  |  |  |  |
| Рабочий стол | Папка может быть перенаправлена независимо | от | всех остальных |  |
| специальных папок. |  |  |  |
|  |  |  |  |
|  |  |  |  |  |
| Мои документы | Особенности и преимущества перенаправления | этой | папки описаны |  |
| ниже. |  |  |  |
|  |  |  |  |
|  |  | | |  |
| Мои | Эта папка может быть перенаправлена независимо от предыдущей папки | | |  |
| документы\ | «Мои документы» или совместно с ней, как это происходит по умолчанию. | | |  |
| Мои рисунки | Именно эта комбинация является рекомендуемой. |  |  |  |
|  |  |  | |  |
| Главное меню | При перенаправлении папки «Главное меню» | ее подпапки всегда | |  |
| перенаправляются вместе с ней. |  |  |  |
|  |  |  |  |
|  |  |  |  |  |

Некоторые из преимуществ, описанных ниже, относятся к перенаправлению любой специальной папки, однако перенаправление папки «Мои документы» может быть особенно удобным, поскольку со временем размер этой папки может увеличиваться.

* При использовании перемещаемого профиля пользователя его частью является только сетевой путь к папке «Мои документы», но не сама папка. Поэтому ее содержимое не нужно копировать и перемещать между клиентом и сервером каждый раз при входе пользователя в систему или его выходе, что делает процессы входа и выхода сравнительно быстрее.
* Даже если пользователь входит в сеть с различных компьютеров, все его документы всегда доступны.
* Технология автономных файлов обеспечивает пользователям доступ к папке «Мои документы» даже при отсутствии подключения к сети. Это особенно полезно для пользователей, использующих мобильные компьютеры. Имеется возможность архивировать данные, 7анящиеся на сервере, при управлении перемещаемыми профилями. Это является более безопасным, поскольку не требуется вмешательство пользователя.
* Системный администратор может устанавливать дисковые квоты с помощью групповой политики, ограничивая дисковое пространство, выделенное пользователю для специальных папок.
* Данные пользователя могут быть перенаправлены на жесткий диск локального компьютера с другого жесткого диска, на котором 7анятся системные файлы ОС. Это может обезопасить пользовательские файлы, если необходимо будет ее переустанавливать.

Кроме всего прочего, в ОС Windows 7 имеется возможность предоставления исключительных прав на специальные папки. Если на вкладке Параметры диалогового окна свойств каждой папки установить флажок Предоставить права монопольного доступа к папке «Мои документы», пользователь и локальная система получают полный контроль над папкой, и никто другой, включая администратора, не будет иметь на нее никаких прав. В противном случае, если этот параметр отключен, то разрешения для папки не изменяются, а используются, применяемые по умолчанию разрешения. Еще одна возможность заключается в том, что на специальные папки могут быть расширены дополнительные разрешения, полный список которых доступен в справке ОС Windows 7.

Установка программного обеспечения является неотъемлемой процедурой при работе с любой ОС. Для этого используется одноименная оснастка «Установка программного обеспечения», которая помогает определить способ установки и сопровождения приложений. Также с ее помощью можно управлять приложением внутри объекта групповой политики посредством службы каталогов Active Directory.

Приложения управляются в одном из двух режимов: назначения или публикации. Приложение назначается, когда необходимо, чтобы оно было установлено на всех узлах сети. Например, требуется, чтобы на всех компьютерах аудитории было установлено одно и тоже приложение. Поскольку объект групповой политики управляет всеми пользователями аудитории, при назначении приложения в объекте групповой политики, оно одновременно объявляется на всех компьютерах, но при этом фактически не устанавливается. Устанавливаются лишь только необходимые данные для создания ярлыка этого приложения в меню Пуск, а в реестре осуществляется связывание расширения его документа с ним самим. При первом выборе приложения на загрузку, а также, если пользователь, не запускавший приложение ранее, выбирает его документ для работы, приложение устанавливается автоматически с одновременным открытием этого документа. Назначенное в системе приложение можно удалить, но оно будет объявлено снова при следующем входе. Если выбрать его в меню Пуск, оно будет повторно автоматически установлено.

Приложение публикуется, если необходимо сделать его доступным для тех пользователей, управляемых объектом групповой политики, кто хочет установить это приложение. При этом у пользователей имеется выбор самостоятельно решать, устанавливать приложение или нет. Например, если приложение публикуется для пользователей, желающих его установить, им следует для этого открыть компонент «Установка и удаление программ» на панели управления и произвести установку. В случае если пользователям не удалось установить приложение с помощью этого компонента, но файлы с соответствующим расширением связаны с приложением, оно будет установлено при первой попытке открыть файл с этим расширением.

Безопасность компьютера, уязвимость системы безопасности, а также различного вида угрозы заботят не только профессионалов в области информационных технологий, но и рядовых пользователей компьютеров. Многие организации и отдельные пользователи имеют постоянные подключения к Интернету, что подвергает их компьютеры рискам заражения вирусами, несанкционированного проникновения, атак на службы и другим угрозам.

Существуют некоторые правила, называемые политиками или параметрами безопасности, которые предназначены для обеспечения защиты ресурсов одного или нескольких компьютеров в сети. Параметры безопасности позволяют контролировать:

* проверку подлинности пользователей при входе в сеть или отдельный узел,
* ресурсы, которые пользователи могут использовать,
* включение и отключение записи действий пользователя или группы в журнале событий,
* принадлежность к группам.

Настраиваются параметры безопасности, используя средства диспетчера настройки безопасности. К этим средствам относятся:

* шаблоны безопасности,
* анализ и настройка безопасности,
* программа командной строки Secedit.exe,
* локальная политика безопасности,
* расширение «Параметры безопасности» для групповой политики.

Расширение «Параметры безопасности» позволяет пользователям изменять настройку безопасности в оснастке «Групповая политика», влияющей, в свою очередь, одновременно на все узлы сети посредством объекта групповой политики. Однако чтобы установить или изменить отдельные параметры безопасности на отдельных компьютерах, используется средство «Локальная политика безопасности», включающее политику аудита, назначение прав пользователя и локальные параметры безопасности.

Чтобы применить несколько параметров безопасности единовременно, имеется возможность определить их с помощью шаблонов безопасности и затем применить к системе с помощью средства «Анализ и настройка безопасности» или программы Secedit.exe (Пуск | Выполнить | Secedit.exe), а также импортировать готовый шаблон в соответствующую локальную или групповую политику.

* заключение следует отметить, что в пакете обновления SP2 для ОС Windows 7 с целью повышения безопасности вводятся некоторые изменения параметров безопасности. Обобщая нововведения, параметры безопасности сгруппированы по соответствующим областям (табл. 16).

**Таблица 16.** Области безопасности ОСWindows7

|  |  |  |
| --- | --- | --- |
| Область безопасности | | **Описание** |
|  |  |  |
| Политики | учетных | Политика паролей, политика блокировки учетной записи и |
| записей |  | политика Kerberos |
|  | |  |
| Локальные политики | | Политика аудита, назначение прав пользователя и параметры |
|  |  | безопасности |
|  | |  |
| Журнал событий | | Параметры журналов событий приложений, системных событий |
|  |  | и событий безопасности |
|  |  |  |
| Группы с | ограниченным | Состав групп с особыми требованиями к безопасности |
| доступом |  |  |
|  | |  |
| Системные службы | | Параметры запуска и разрешения для системных служб |
|  |  |  |
| Реестр |  | Разрешения для разделов реестра |
|  | |  |
| Файловая система | | Разрешения для файлов и папок |
|  |  |  |

**Содержание задания**

Прежде чем непосредственно перейти к ознакомлению с возможностями изучаемой оснастки, следует обратить внимание на имеющиеся в системе способы ее открытия в изолированном виде. Имеется возможность открыть оснастку через меню Пуск | Выполнить. Для этого необходимо ввести gpedit.msc и нажать Enter для ввода. Кроме того, загрузка оснастки возможна в среде командной оболочки, различные варианты которой отображены ниже (табл. 17). Поэкспериментируйте с имеющимися возможностями загрузки изолированной оснастки «Групповая политика».

**Таблица 17.** Варианты загрузки групповой политики посредством командной оболочки

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | **Пример команды** | **Описание** | | |  |  |  |
| п.п. |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | | |  | |  |
|  |  | редактирование | | | групповой | |  |
| 1 | gpedit.msc /gpcomputer:»Имя\_компьютера» | политики | |  | локального | |  |
|  |  | компьютера. | | |  |  |  |
|  |  |  | | |  | |  |
|  |  | редактирование | | | локального | |  |
|  | gpedit.msc /gpcomputer:»Имя\_компьютера.WingTip | объекта | | групповой политики | | |  |
| 2 | на | локальном | | компьютере, | |  |
| Toys.com» |  |
|  | имя | которого | | задается | в |  |
|  |  |  |
|  |  | формате DNS. | | |  |  |  |
|  |  |  | | |  | |  |
|  | gpedit.msc /gpobject:»LDAP://CN={31B2F340016D- | редактирование | | | объекта | |  |
|  | 11D2-945F00C04FB984F9},CN=Policies,CN=Syste | групповой | | политики | | с |  |
| 3 | m,DC=WingTipToys,DC=com» в фигурных скобках | применением Active Directory. | | | |  |  |
|  | {16-байтное число} — глобальный уникальный |  |  |  |  |  |  |
|  | идентификатор GUID |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

1. Загрузите пользовательскую консоль администрирования, созданную в задании 39, с возможностью ее редактирования.
2. Добавьте оснастку «Редактор объекта групповой политики» в корень консоли администрирования, выбрав в поле Объекта групповой политики значение Локальный компьютер.
3. Откройте поочередно все ветви дерева консоли в узле Политика «Локальный компьютер» и изучите где и какие параметры групповой политики располагаются. Обратите внимание на то, что некоторые параметры находятся в состоянии Включено, другие, напротив — Отключено или Не определено (Не задано).
4. В левой части окна консоли выберите «Политика Локальный компьютер | Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователей / Параметры безопасности».
5. Изучите локальные политики Назначение прав пользователя и Параметры безопасности.
6. Сохраните и закройте консоль администрирования MMC.

При выполнении пункта 6 используйте следующие инструкции:

* последовательно перебирая каждую из локальных политик, изучите ее содержимое, принадлежность к пользователю, а также состояние, в котором она находится,
* запишите полученную информацию в отчет, заполнив табл. 18.
* сделайте вывод о проделанной работе и запишите его в отчет.

**Таблица 18.** Локальная политика безопасности ОС Windows7

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | **Политика** |  |  | **Привилегией** |  |  |  |
|  |  |  |  | **Состояние** |  |
| п.п. | **Название** | **описание** |  | **обладает** |  |  |
|  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| **1** | **Изменение** | **Определяет,** | **какие** | **Администратор** |  | **Включено** |  |
|  | **системного** | **пользователи** | **и** | **Опытный** |  |  |  |
|  | **времени** | **группы** | **могут** | **пользователь** |  |  |  |
|  |  | **изменять время и** | |  |  |  |  |
|  |  | **дату компьютера.** | |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| n |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**Задание 9. Возможности оснастки «Групповая политика» при настройке локального узла**

Как утверждалось ранее, с помощью параметров узла Конфигурация компьютера устанавливаются политики, которые применяются к компьютеру независимо от того, кто его использует для входа в сеть, в то время как, с помощью параметра Конфигурация пользователя устанавливаются политики, которые применяются к каждому пользователю, работающему на компьютере.

Таким образом, существует ряд параметров групповой политики предназначенных исключительно для изменений, направленных на создание специальных настроек среды пользователя ОС Windows 7, в частности, для придания системе уникального вида. В качестве примера, с помощью групповой политики можно удалить значки с рабочего стола, изменить содержимое меню Пуск и упростить структуру панели управления.

**Содержание задания**

1. Загрузите пользовательскую консоль администрирования, созданную ранее, с возможностью ее редактирования.
2. В левой части окна консоли выберите «Политика Локальный компьютер | Конфигурация пользователя | Административные шаблоны | Панель задач и меню «Пуск» / Панель управления / Рабочий стол». Изучите параметры политик | Административные шаблоны | Панель задач и меню «Пуск» / Панель управления / Рабочий стол.
3. Выберите любые пять параметров в каждой из политик Панель задач и меню «Пуск» / Панель управления / Рабочий стол. Измените выбранные параметры на противоположные, перезагрузите компьютер и отметьте полученные визуальные изменения графического интерфейса.
4. Сохраните и закройте консоль администрирования MMC.

При выполнении пункта 3 используйте следующие инструкции:

* самостоятельно последовательно выбирая политики указанных административных шаблонов, в общем количестве не менее десяти, измените их состояние, делая его активным,
* исследуйте влияние смены состояния на внешний вид соответствующего элемента графического интерфейса ОС Windows 7,
* запишите полученную информацию в отчет, заполнив табл. 19.
* сделайте вывод о проделанной работе и запишите его в отчет.
* продемонстрируйте преподавателю конечный результат изменения параметров административных шаблонов, применяемых для настройки уникального вида элементов графического интерфейса.

**Таблица 19.** Настройка некоторых административных шаблонов

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  | **Административный шаблон** | |  |  |  |
|  |  | № |  |  |  |  |  |  |
|  |  |  |  |  | **Результат при активации политики** |  |
|  |  | п.п. |  | **Название** | **Описание** | |  |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  | **шаблона** | **политики** | |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | 1 |  | Рабочий стол | Не | показывать | При изменении состояния политики в |  |
|  |  |  |  |  | значок | Internet | положениеВключенозначокIE |  |
|  |  |  |  |  | E7lorer (IE) | | убирается с рабочего стола и панели |  |
|  |  |  |  |  |  |  | быстрого запуска |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  | n |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**Задание 10. Возможности оснасток, предназначенных для диагностики, мониторинга, настройки и оптимизации**

* широком смысле аудитом называется регистрация каких-либо действий, процессов или событий, предназначенная для обеспечения комплексной безопасности чего-либо. В частности, средства аудита в среде ОС Windows 7 предназначены для отслеживания действий пользователей путем регистрации системных событий определенных типов в журнале безопасности сервера или рабочей станции. Кроме того, отображение и фиксация системных событий необходимы для определения злоумышленников или попыток поставить под угрозу данные операционной системы. Примером события, подлежащего аудиту, является неудачная попытка доступа к системе.

Наиболее общими типами событий, подлежащих аудиту в ОС, являются:

* доступ к таким объектам, как файлы и папки;
* управление учетными записями пользователей и групп;
* вход пользователей в систему и выход из нее.

Чтобы обеспечить возможность аудита в среде ОС Windows 7, сперва необходимо выбрать политику аудита, указывающую категории событий аудита, связанных с безопасностью. При инсталлировании ОС все категории аудита по умолчанию выключены; включая их последовательно администратор может создать политику аудита, удовлетворяющую всем требованиям организации.

К числу категорий событий, предназначенных для контроля, относятся:

* аудит событий входа в систему;
* аудит управления учетными записями;
* аудит доступа к службе каталогов;
* аудит входа в систему;
* аудит доступа к объектам;
* аудит изменения политики;
* аудит использования привилегий;
* аудит отслеживания процессов и системных событий.

В частности, если выбран аудит доступа к объектам как часть политики аудита, необходимо включить либо категорию аудита доступа к службе каталогов (для аудита объектов на контроллере домена), либо категорию аудита доступа к объектам (для аудита объектов на рядовой сервер или рабочую станцию).Кроме того, с целью уменьшения риска угроз системной безопасности в целом администратор должен предпринять следующие базовые шаги, направленные на обеспечение аудита в системе. Основные события аудита и угрозы безопасности, отображаемые при помощи этого события, сведены в табл. 20.

**Таблица 20.** Основные события аудита в ОС Windows7

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № | **Событие аудита** | **Потенциальная** | |  |
| п.п. | **угроза** |  |  |
|  |  |  |
|  |  |  |  |  |
|  | Аудит отказов входа/выхода. | Случайный | взлом |  |
| 1 |  | пароля |  |  |
|  |  |  | |  |
| 2 | Аудит успехов входа/выхода. | Вход с украденным | |  |
|  | паролем |  |  |
|  |  |  |  |
|  |  |  |  |  |
|  | Аудит успехов использования привилегий, управления | Неправильное |  |  |
| 3 | пользователямиигруппами,измененийполитик | использование |  |  |
| безопасности, перезагрузки, выключения и системных | привилегий |  |  |
|  |  |  |
|  | событий. |  |  |  |
|  |  |  |  |  |
|  | Аудит успехов и отказов событий доступа к файлам и | Неправильный | доступ |  |
| 4 | объектам. Аудит успехов и отказов диспетчера файлов в | к важным файлам | |  |
| доступе подозрительным пользователям или группам к |  |  |  |
|  |  |  |  |
|  | важным файлам для чтения и записи. |  |  |  |
|  |  |  |  |  |
|  | Аудит успехов и отказов событий доступа к принтерам и | Неправильный | доступ |  |
| 5 | объектам. Аудит успехов и отказов диспетчера печати в | к принтерам |  |  |
| доступе подозрительным пользователям или группам к |  |  |  |
|  |  |  |  |
|  | принтерам. |  |  |  |
|  |  |  | |  |
|  | Аудит успехов и отказов доступа для записи к | Эпидемия вирусов | |  |
| 6 | программным файлам с расширениями .exe и .dll. Аудит |  |  |  |
| успехов и отказов для отслеживания процессов в системе |  |  |  |
|  |  |  |  |
|  | при запуске подозрительных программ. |  |  |  |
|  |  |  |  |  |

Формирование политики аудита объектов в системе осуществляется посредством оснастки «Групповая политика»; в частности, с ее помощью устанавливается и настраиваются параметры политики аудита.

**Содержание задания**

1. Откройте консоль администрирования и создайте в оснастке новые задачи «Сведения о системе», «Диагностика DirectX» и «Диспетчер задач», вызовите соответствующие системные модули (указанные в задании 34) для выполнения задач диагностирования и мониторинга ОС Windows 7. Убедитесь в работоспособности этих задач.
2. Локально добавьте на открытую консоль администрирования системную оснастку «Групповая политика».
3. В дереве консоли «Политика «Локальный компьютер» щелкните манипулятором мышь по папке «Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Политика аудита» для настройки локальных политик аудита.
4. Настройте политики аудита. Для этого в области сведений дважды щелкните на политике аудита, для которой необходимо изменить параметры аудита и установите один или оба флажка («успех» или «отказ») для успешных или неуспешных системных событий, которые необходимо регистрировать. Повторите действия указанные в текущем пункте секции для других политик аудита в случае необходимости.
5. Настройте аудит файлов и папок. Для этого измените параметры «успех» или «отказ» категории событий «Аудит доступа к объектам». Укажите файлы или папки для аудита, выполнив следующие действия:

* на вкладке «Безопасность» команды «Свойства» файла или папки нажмите кнопку «Дополнительно»,
* на вкладке «Аудит» нажмите кнопку «Добавить»,
* в диалоговом окне «Выбор: пользователь, компьютер или группа» выберите имя пользователя или группы, для действий которых требуется производить аудит файлов и папок, и нажмите кнопку OK для подтверждения выбора;
* в появившемся диалоговом окне «Элемент аудита» в группе «Доступ» установите флажки «успех», «отказ» или оба эти флажка одновременно напротив действий, для которых требуется провести аудит,
* выберите из выпадающего меню «Применить:» опцию «Для этой папки и ее подпапок» (или любую другую опцию на Ваш выбор), а затем нажмите кнопку OK и Примерить для подтверждения ввода.

Если указанные выше действия выполнить не удалось по причине отсутствия вкладки «Безопасность» в «Свойствах» объекта, выполните следующее:

* в дереве консоли «Политика «Локальный компьютер» щелкните манипулятором мышь по папке «Конфигурация пользователя | Административные шаблоны | Компоненты Windows | Проводник»;
* в области сведений дважды щелкните на «Удалить вкладку «Безопасность», измените системный параметр на «Отключено» на одноименной вкладке и подтвердите выбор, кликнув OK;

1. выберите команду Панель управления в меню Пуск, откройте компонент «Свойства папки» на панели управления, дважды щелкнув по нему мышью, и на вкладке «Вид» в группе «Дополнительные параметры | Файлы и папки» снимите флажок «Использовать простой общий доступ к файлам (рекомендуется)».Не закрывая консоль администрирования ММС, сохраните ее.

При выполнении заданий секции используйте следующие инструкции:

* перенесите последовательность выполняемых действий по каждому из пунктов 1-5 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
* сделайте вывод о проделанной работе и запишите его в отчет.

**Задание 11. Возможности оснастки «Просмотр событий»**

Поскольку, аудит предполагает регистрацию различного рода системных событий (табл. 21), имеющих место в операционной среде, их регистрация в ОС Windows 7 осуществляется в журналах трех основных типов, описание которых представлено после таблицы.

* журнале приложений содержатся данные, относящиеся к работе приложений. Записи этого журнала создаются самими приложениями. События, вносимые в журнал, определяются разработчиками соответствующих приложений.

Журнал безопасности содержит записи о таких событиях, как успешные и безуспешные попытки доступа в ОС, а также о событиях, относящихся к использованию системных ресурсов. В частности, после разрешения аудита входа в систему сведения обо всех попытках входа заносятся в журнал безопасности. Именно в этом журнале аккумулируются данные по системным событиям, аудит которых был настроен в предыдущей секции учебного задания.

* журнале системы содержатся события системных компонентов ОС. Так, например, в журнале системы регистрируются сбои при загрузке драйвера или других программных компонентов в момент запуска системы.
* дополнение к существующим ОС Windows 7 имеет в своем распоряжении еще два журнала: службы каталогов и службы репликации файлов, запись событий в которые выполняется в случае, если компьютер настроен в качестве контроллера домена.

**Таблица 21.** Типы системных событий в ОС Windows7

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| № | **Тип события** | **Описание** |  |  |  |  |  |
| п.п. |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  | | | | |  |
|  |  | Возникает при серьезных трудностях, связанных с потерей | | | | |  |
| 1 | Ошибка | данных или функциональности ОС (например, при сбое | | | | |  |
|  |  | загрузки службы в момент ее запуска). | | |  |  |  |
|  |  |  | | | | |  |
|  |  | Возникает при событии, которое в момент записи в журнал не | | | | |  |
| 2 | Предупреждение | было существенным, но может привести к ошибкам в будущем | | | | |  |
|  |  | (например, если на диске осталось мало свободного места). | | | | |  |
|  |  |  | | | | |  |
|  |  | Возникает при событии, описывающее удачное завершение | | | | |  |
| 3 | Уведомление | действия приложением, драйвером или службой (например, | | | | |  |
|  |  | после успешной загрузки драйвера). | | |  |  |  |
|  |  |  | | | | |  |
|  |  | Возникает при событии, которое соответствует успешно | | | | |  |
| 4 | Аудит успехов | завершенному | действию, | связанному | с | поддержкой |  |
| безопасности ОС (например, в случае успешного входа | | | | |  |
|  |  |  |
|  |  | пользователя в систему). | |  |  |  |  |
|  |  |  | | | | |  |
|  |  | Возникает при событии, которое соответствует неудачно | | | | |  |
| 5 | Аудит отказов | завершенному | действию, | связанному | с | поддержкой |  |
| безопасности ОС (например, в случае неудачной попытки | | | | |  |
|  |  |  |
|  |  | доступа пользователя к сетевому диску). | | |  |  |  |
|  |  |  |  |  |  |  |  |

* журнале службы каталогов содержатся события, заносимые службой каталогов ОС Windows 7. Например, проблемы соединения между сервером и общим каталогом записываются в этот журнал.

Журнал службы репликации файлов содержит записи о системных событиях, внесенных службой репликации файлов ОС Windows 7. В этот журнал записываются неудачи при репликации файлов, а также события, которые происходят пока контроллеры домена обновляются данными об изменениях из общей папки Sysvol, где 7анится серверная копия общих файлов, реплицируемых между всеми контроллерами домена.

Кроме того, существует журнал DNS-сервера, в который записываются сообщения об системных событиях, зарегистрированных службой DNS. В этот журнал записываются события, связанные с разрешением DNS-имен IP-адресам.

* ОС Windows 7 за регистрацию системных событий в описанных выше журналах отвечает специальная служба, называемая службой журнала событий, которая загружается автоматически при старте системы. Эта служба контролирует ведение журналов и осуществляет внесение в них соответствующих записей системных событий в реальном масштабе времени. При этом любой пользователь может просматривать журналы приложений и системы, однако журналы безопасности доступны только системному администратору, который предварительно должен настроить параметры системных событий аудита (табл. 20), воспользовавшись компонентом «Групповая политика».

**Содержание задания**

1. Локально добавьте на открытую консоль администрирования новую системную оснастку «Просмотр событий».
2. В дереве консоли щелкните манипулятором мышь по оснастке «Просмотр событий» и обратите внимание на появившиеся три журнала и их текущие размеры в области сведений справа. Последовательно перебирая журналы приложений, безопасности и системы, отметьте в них наличие всех указанных выше типов системных событий (табл. 20). При этом обратите внимание на то, что такие типы событий как аудиты отказов и успехов присущи только журналу безопасности, который был Вами настроен в предыдущей секции. Остальные типы событий встречаются как в журнале приложений, так и в журнале системы.
3. Воспользовавшись меню «Вид» изучаемой оснастки, отфильтруйте:

* в журнале приложений событие «Уведомление» за прошедшее время,
* в журнале безопасность событие «Аудит отказов» за IV квартал,
* в журнале система событие «Ошибка» за последнюю неделю, с сортировкой по дате «от старых к новым».

1. В окне журнала событий системы удалите столбцы «Пользователь», «Компьютер» и «Категория», оставив остальные.
2. Воспользовавшись системой поиска, найдите событие типа «Предупреждение» с кодом 1003 от источника DHCP в журнале событий системы.
3. Создайте собственный журнал событий, содержащий только сведения об ошибках приложений и программ. Установите максимальный размер этого журнала в 128 Кб и возможность затирания старых событий по необходимости. Сохраните созданный журнал в двоичном виде с расширением .evt.
4. Создайте инструмент для регистрации событий аудита любого компьютера рабочей группы или домена и осуществите просмотр системных событий другого узла локальной сети с его помощью.
5. Не закрывая консоль администрирования ММС, сохраните ее.

При выполнении заданий секции используйте следующие инструкции:

* перенесите последовательность выполняемых действий по каждому из пунктов 1-6 в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),
* сделайте вывод о проделанной работе и запишите его в отчет.