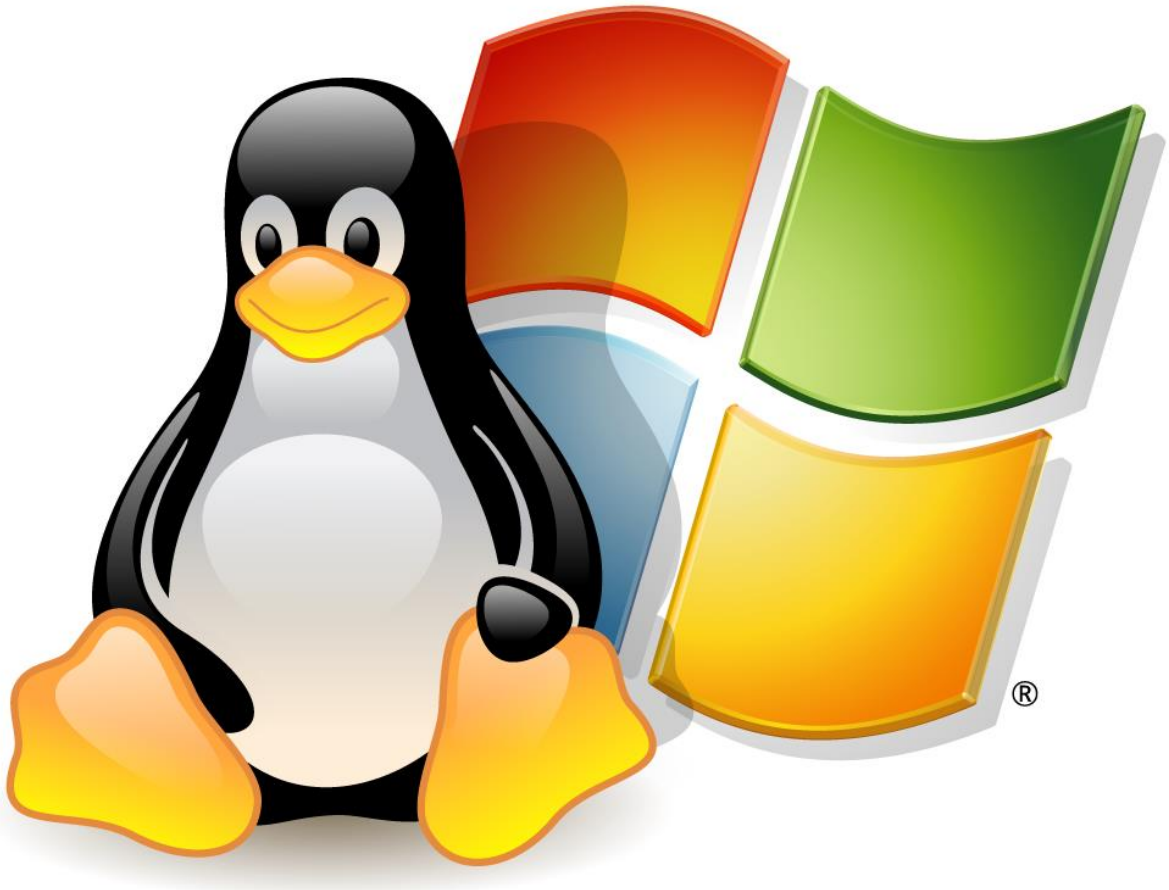
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Д.О. Пахмурин

ОПЕРАЦИОННЫЕ СИСТЕМЫ ЭВМ

Учебно-методическое пособие к практическим занятиям



Томск – 2015

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ (ТУСУР)

Кафедра промышленной электроники

Д.О. Пахмурин

ОПЕРАЦИОННЫЕ СИСТЕМЫ ЭВМ

Учебно-методическое пособие
к практическим занятиям для студентов
очной формы обучения по направлению
11.03.04 – Электроника и наноэлектроника
(профиль "Промышленная электроника")

2015

Пахмурин Д.О.
Операционные системы ЭВМ: Учебно-методическое пособие к практическим занятиям. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2015. – 155 с.

Приведены методические указания для выполнения практических занятий по дисциплине "Операционные системы ЭВМ", определена тематика и порядок их выполнения.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Данные методические указания являются дополнением к учебному пособию "Операционные системы ЭВМ" для студентов очной формы обучения. Они являются необходимыми для практической подготовки современного инженера к деятельности по администрированию операционных систем.

Целью методических указаний является познакомить студентов с основными моментами в управлении операционными системами и привитие им соответствующих практических знаний в сфере компьютерных технологий. В современном мире без достаточно полноценного обучения работе с информацией, с принципами функционирования компьютерного оборудования не возможна качественная разработка каких-либо серьезных технических проектов.

Более глубокие практические знания будут даны студентам в рамках лабораторных работ, руководство по выполнению которых будет издано в виде отдельного учебно-методического пособия в ближайшее время.

1. Изучение основных принципов организации и построения консоли администрирования MMC в ОС Windows XP.

Цель работы: Изучить основные принципы организации и построения консоли администрирования, а также базовые возможности некоторых инструментов системного администратора ОС Windows XP.

1.1. Краткие теоретические сведения

Консоль управления Microsoft Management Console, сокращенно MMC является инструментом создания, сохранения и открытия средств администрирования (называемых консолями MMC), которые управляют оборудованием, программными и сетевыми компонентами операционной системы (ОС), иными словами, это основа администрирования любой ОС, в частности ОС Windows XP.

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, виды 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 практических и лабораторных работ по применению различных оснасток.

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 показывает 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**,
- 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, и **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 ММС 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 **/а**,

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

Очевидно, что загрузка консоли ММС 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 соответствующая работа.

Прежде чем создавать новую консоль ММС, 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 ММС находится на Web-узле корпорации Майкрософт (http://www.microsoft.com).

В практической работе предполагается ознакомление с основными принципами организации и построения консоли администрирования ММС.

1.2. Подготовка к выполнению практической работы

Перед началом выполнения практической работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню (**Пуск |Справка и поддержка**);

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с 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").

1.3. Порядок выполнения практической работы

Для выполнения практической работы необходимо запустить виртуальную машину с гостевой ОС Windows XP.

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 созданной ранее консоли администрирования:

A. запуск из командной строки, используя синтаксис:

Mmc *путь\имя_файла.msc* /**a**,

где параметр:

путь\имя_файла.msc – запускает консоль MMC с одновременным открытием файла сохраненной консоли с именем имя_файла.msc (Таблица 1.1). 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 XP 64-Bit Edition.

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

Дополнительная информация по данной команде доступна одноименном разделе справки ОС Windows XP (**Пуск | Справка и поддержка**). Справку также можно получить, набрав в окне командной оболочки строку **Mmc /?** и нажав **Enter** для ввода.

Таблица 2.1. Список штатных консолей MMC, применяемых в ОС Windows XP с целью администрирования, мониторинга, оптимизации и аудита

№ п/п.	Файл консоли MMC	Описание
1.	dfrg.msc	Дефрагментация дисков
2.	devmgmt.msc	Диспетчер устройств
3.	gpedit.msc	Групповая политика
4.	ntmsoprq.msc	Запрос операторов съемных ОЗУ
5.	wmimgmt.msc	Инфраструктура управления
6.	secpol.msc	Локальные параметры безопасности
7.	lusrmgr.msc	Локальные пользователи и группы
8.	fsmgmt.msc	Общие папки
9.	perfmon.msc	Производительность
10.	eventvwr.msc	Просмотр событий
11.	rsop.msc	Результирующая политика
12.	certmgr.msc	Сертификаты
13.	services.msc	Службы
14.	ciadv.msc	Служба индексирования
15.	ntmsmgr.msc	Съемные ЗУ
16.	diskmgmt.msc	Управление дисками
17.	compmgmt.msc	Управление компьютером

Примечание. Файлы консоли MMC расположены в системном каталоге C:\WINDOWS\system32\ или %Systemroot%\system32\. Пример запуска консоли **dfrg.msc** из командной строки: **mmc** %Systemroot%\system32\dfrg.msc.

В. Запуск из файлового менеджера Проводник ОС Windows XP:

– 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**.

II. Настройка параметров консоли администрирования ММС предназначена для ее конфигурирования с целью придания ей уникального вида.

Задание № 1.1. Изучить возможности изменения параметров и способы настройки консоли администрирования ММС на конкретных примерах.

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

1. В меню **Консоль** выберите команду **Параметры**.

2. На вкладке **Консоль** в поле названия введите новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

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 **Применить** для подтверждения.

4. На вкладке **Консоль** из списка **Режим консоли** выберите пользовательский режим с полным доступом, в котором будет открываться консоль ММС при ее непосредственном запуске.

5. Для установленного в предыдущем пункте режима выполните указанные ниже действия:

– запретите изменение консоли ММС при ее непосредственном запуске, установив флажок "**Не сохранять изменения для этой консоли**",

– сделайте активным диалоговое окно **Вид | Настройка вида** консоли ММС при запуске, установив флажок **"Разрешить пользователю настраивать вид консоли"**.

6. Если необходимо удалить файлы, содержащие параметры отображения файлов консоли, на вкладке **Очистка диска** нажмите кнопку **Удалить файлы**.

7. Сохраните окончательно сконфигурированную консоль администрирования ММС, 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 C:\Documents and Settings\student\Главное меню\Программы\Администрирование\.

8. Закройте сконфигурированную и сохраненную консоль администрирования MMC.

В файловом менеджере Проводник ОС Windows XP выполните следующие инструкции:

– наведите манипулятором мышь на сохраненный файл консоли администрирования MMC и, дважды кликнув на нем, запустите консоль,

– откройте диалоговое окно **Вид | Настроить** и, изменяя положение флажков, обратите внимание на получаемый результат,

– изменив вид консоли MMC приемлемым образом, кликните **ОК** 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.

III. Добавление различных элементов и компонентов к дереву консоли администрирования MMC предназначено для конфигурирования консоли с целью придания ей уникальных функций и оптимизации ее работы в целом.

Основным, интегрируемым на консоль компонентом, как уже упоминалось, является оснастка. Оснастки существуют двух видов: **изолированные** и **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.

В 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 XP (**Пуск | Справка и поддержка**) в разделе **Общее представление о MMC \ Консоль MMC в авторском режиме \ Оснастки \ Создание консолей**.

Задание № 1.2. Исследовать процесс добавления различных элементов и компонентов к дереву консоли администрирования MMC на конкретных примерах.

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 из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.

4. 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**.

5. 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.

6. 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.

7. Нажмите **Готово**, **Закрыть** и затем кликните **ОК** для подтверждения ввода.

8. 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**,
- Нажмите **ОК**.

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.

9. Не закрывая консоль администрирования ММС, сохраните ее, выбрав команду **Сохранить** в меню **Консоль**.

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

10. В меню **Консоль** выберите команду **Добавить или удалить оснастку**.

11. 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.

12. Среди **Доступных расширений** оснастки **Службы** удалите флажок с расширения **Расширенный вид** (предварительно сняв флажок **Добавить все разрешения**) и отметьте, к чему привело это действие. Повторите аналогичные действия с другими расширениями данной оснастки и изучите получаемый результат.

13. Не закрывая консоль администрирования ММС, 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.

Следующим элементом, необходимым в ряде случаев администрирования и предназначенным, в том числе, для удобства отображения информации, является новый вид панели задач. Для добавления видов панелей задач и собственно задач в авторском режиме выполните следующее:

1. Создайте новую **Консоль** управления ММС одним из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. Добавьте оснастку **Службы** в корень консоли ММС.

4. В дереве консоли кликните манипулятором мышь на этой оснастке.

5. В меню **Действие** или кликнув правой кнопкой манипулятора на оснастке, выберите команду **Новый вид панели задач**.

6. Следуйте инструкциям **"Мастера создания вида панели задач"**, чтобы добавить на консоль новую панель вида.

7. 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"**.

8. Следуйте инструкциям "**Мастера создания новой задачи"**, чтобы добавить на консоль новую задачу к существующей панели вида.

9. 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**.

10. На вкладке **Задачи** нажмите кнопку **Создать**.

11. Повторите инструкции пункта 7 настоящего задания.

12. Не закрывая консоль администрирования ММС, сохраните ее.

Измените вид панели задач сохраненной консоли администрирования ММС, 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 отобразить 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 **ОК** для подтверждения ввода,

– изучите полученный результат,

– сделайте вывод о проделанной.

Важной особенностью при построении и организации консоли администрирования ММС является возможность добавления элементов и компонентов дерева консоли в виде списка ярлыков в меню **"Избранное"**. Для добавления элемента или компонента в авторском режиме выполните следующее:

1. Создайте новую Консоль управления ММС одним из описанных в **пункте I** текущего учебного задания способов.

2. Задайте данной консоли новый заголовок, содержащий **номер группы и фамилии студентов**, выполняющих данную работу.

3. В дереве консоли кликните элемент или компонент (в нашем случае это оснастка), который нужно добавить в список "Избранное".

4. 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.

5. Выберите в меню **Избранное** команду **Добавить в избранное**.

6. 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 **ОК** для ввода,

– в поле **Имя папки** введите имя, под которым будет добавлен элемент, кликните **ОК** для подтверждения ввода.

7. Не закрывая консоль администрирования ММС, сохраните ее.

Упорядочите "Избранное" сохраненной консоли администрирования ММС, выполнив следующие действия:

– добавьте новую папку, введя ее имя в соответствующее поле и кликнув **ОК** для подтверждения ввода,

– переместите элемент, созданный в **пункте 5** настоящего задания, в новую, только что созданную, папку и кликните **ОК** 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.

2. Механизмы резервного копирования данных в операционной системе Windows XP

Цель работы: Получить навыки архивирования и восстановления системы, используя стандартные утилиты Windows XP. Решить задачи сетевого администратора, связанные с сохранением, архивированием информации, и ее последующим восстановлением.

2.1. Краткие теоретические сведения

Ни один носитель информации не является абсолютно надежным, из строя может выйти любое устройство хранения данных, и данные могут быть потеряны. Кроме аппаратных сбоев возможна также потеря данных по причине действия вредоносных программ (вирусы и т.п.). А самая распространенная причина порчи или удаления данных – ошибки пользователей (как обычных, так и администраторов), которые могут по ошибке удалить или перезаписать не тот файл.

По этой причине возникает необходимость регулярного создания резервных копий информации – файлов с документами, баз данных и состояния операционной системы.

Системы семейства Windows имеют встроенный инструмент создания резервных копий – утилиту *ntbackup*. Данная утилита позволяет сохранять резервные копии на самых различных носителях – ленточных накопителях, магнитооптических дисках, жестких дисках (как на локальных дисках данного сервера, так и на сетевых ресурсах, размещенных на других компьютерах сети). В версии системы Windows XP реализован механизм т.н. теневых копий *Shadow Copy*, который заключается в том, что в начале процедуры архивации система делает моментальный "снимок" архивируемых файлов и уже после этого создает резервную копию из этого снимка. Данная технология позволяет архивировать файлы, которые в момент запуска утилиты *ntbackup* были открыты пользователями.

Сетевой администратор должен совместно с пользователями определить те данные, которые нужно регулярно архивировать, спланировать ресурсы, необходимые для создания резервных копий, составить расписание резервного копирования, настроить программу резервного копирования и планировщик заданий для автоматического создания резервных копий. Кроме этого, в задачу сетевого администратора входит также регулярное тестирование резервных копий

и пробное восстановление данных из резервных копий (чтобы вовремя обнаружить возникающие проблемы в создании резервных копий).

Архивирование и восстановление файловых ресурсов. Базовые понятия службы резервного копирования

Все операции по созданию резервных копий и восстановлению данных в ОС семейства Windows осуществляются утилитой *ntbackup*. Рассмотрим основы резервного копирования файловых ресурсов. Каждый файл, хранящийся на диске компьютера, независимо от типа файловой системы, имеет атрибут *archive*, который в Свойствах файла отображается как "*Файл готов для архивирования"* (откройте Свойства файла и нажмите кнопку "*Дополнительно"*). Если в Свойствах файла вручную убрать галочку у этого атрибута, то при любом изменении в файле операционная система автоматически снова установит этот атрибут. На использовании изменений данного атрибута основаны все используемые в системе Windows методики резервного копирования.

Типы резервного копирования

Утилитой *ntbackup* можно создавать резервные копии различных типов. Рассмотрим их отличительные особенности и различные варианты их применения.

– *Обычный (Normal)* При выполнении данного типа архивирования утилита *ntbackup* архивирует все файлы, отмеченные для архивации, при этом у всех заархивированных файлов очищается атрибут "Файл готов для архивирования". Данный вид архивирования необходим для создания еженедельных полных резервных копий каких-либо больших файловых ресурсов. Если в компании или организации имеются достаточные ресурсы, то можно ежедневно осуществлять полное архивирование данных.

– *Разностный (Differential)* При выполнении Разностного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут "Файл готов для архивирования", при этом данный атрибут не очищается. Использование Обычного и Разностного архивирования позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Например, если раз в неделю (как правило, в выходные дни) создавать Обычные копии, а в течение недели ежедневно (как правило, в ночное время) – Разностные, то получается выигрыш в объеме носителей для резервного копирования. При такой комбинации архивирования "Обычный + Разностный" процесс восстановления данных в случае утери

информации потребует выполнения двух операций восстановления – сначала из последней Полной копии, а затем из последней Разностной резервной копии.

– *Добавочный (Incremental)* При выполнении Добавочного архивирования утилита *ntbackup* из файлов, отмеченных для архивирования, архивирует только те, у которых установлен атрибут "Файл готов для архивирования", при этом данный атрибут очищается. Использование Обычного (раз в неделю по выходным) и Добавочного (ежедневно в рабочие дни) архивирования также позволяет сэкономить пространство на носителях с резервными копиями и ускорить процесс создания ежедневных копий. Но процесс восстановления данных при использовании комбинации "Обычный + Добавочный" уже будет выполняться иначе: в случае утери информации для восстановления данных потребуется сначала восстановить данные из последней Полной копии, а затем последовательно из всех Добавочных копий, созданных после Полной копии.

– *Копирующий (Copy)* При таком типе архивирования утилита *ntbackup* заархивирует все отмеченные файлы, при этом атрибут "Файл готов для архивирования" остается без изменений.

– *Ежедневный (Daily)* Ежедневный тип архивирования создает резервные копии только тех файлов, которые были модифицированы в день создания резервной копии.

Два последних типа не используются для создания регулярных резервных копий. Их удобно применять в тех случаях, когда с какой-либо целью нужно сделать копию файловых ресурсов, но при этом нельзя нарушать настроенные регулярные процедуры архивирования.

Разработка и реализация стратегии резервного копирования. Понятие плана архивации

Создание и реализация плана архивации и восстановления информации – непростая задача. Сетевому администратору надо определить, какие данные требуют архивации, как часто проводить архивацию и т. д. При создании плана ответьте на следующие вопросы:

– Насколько важны данные? Этот критерий поможет решить, как, когда и какую информацию архивировать. Для критичной информации, например, для баз данных, следует создавать избыточные архивные наборы, охватывающие несколько периодов архивации. Для менее важной информации, например, для текущих

пользовательских файлов, сложный план архивации не нужен, достаточно регулярно сохранять их и уметь легко восстанавливать.

– К какому типу относится архивируемая информация? Тип информации поможет определить необходимость архивации данных: как и когда данные должны быть сохранены.

– Как часто изменяются данные? Частота изменения влияет на выбор частоты архивирования. Например, ежедневно меняющиеся данные необходимо сохранять каждый день.

– Нужно ли дополнить архивацию созданием теневых копий? При этом следует помнить, что теневая копия — это дополнение к архивации, но, ни в коем случае, не ее замена.

– Как быстро нужно восстанавливать данные? Время – важный фактор при создании плана архивации. В критичных к скорости системах нужно проводить восстановление очень быстро.

– Какое оборудование оптимально для архивации и есть ли оно у вас? Для своевременной архивации вам понадобится несколько архивирующих устройств и несколько наборов носителей. Аппаратные средства архивации включают ленточные накопители (это наименее дорогой, но и самый медленный тип носителя), оптические диски и съемные дисковые накопители.

– Кто отвечает за выполнение плана архивации и восстановления данных? В идеале и за разработку плана, и собственно за архивацию и восстановление должен отвечать один человек.

– Какое время оптимально для архивации? Архивация в период наименьшей загрузки системы пройдет быстрее, но не всегда возможно провести ее в удобные часы. Поэтому с особой тщательностью архивируйте ключевые данные.

– Нужно ли сохранять архивы вне офиса? Хранение архивов вне офиса – важный фактор на случай стихийного бедствия. Вместе с архивами сохраните и копии ПО для установки или переустановки ОС.

Для построения правильной и эффективной системы резервного копирования необходимо детально изучить и задокументировать все файловые ресурсы, используемые в компании, а затем тщательно спланировать стратегию резервного копирования и реализовать ее в системе. Для планирования стратегии необходимо ответить на следующие вопросы:

– какие именно ресурсы будут архивироваться;

– минимальный промежуток времени для восстановления данного ресурса при возникновении аварии;

– какой объем данных будет архивироваться;

– какова емкость носителей для хранения резервных копий и скорость записи на эти носители;

– сколько времени будет занимать архивирование каждого ресурса;

– как часто будет производиться архивация каждого ресурса;

– если резервные копии записываются на ленты, то как часто будет производиться перезапись лент;

– по какому графику будет производиться тестовое восстановление данных.

При ответе на эти вопросы будет спланирована потребность в количестве и емкости накопителей и устройств для выполнения резервных копий, требования к пропускной способности сети для создания резервных копий, график выполнения резервного копирования, план восстановления на случай аварии.

Выбор архивных устройств и носителей

Определив, какие данные и как часто архивировать, можно выбрать аппаратные средства архивации и необходимые носители. Инструментов для архивации данных множество. Одни быстрые и дорогие, другие — медленные и надежные. Выбор подходящего оборудования для организации зависит от многих факторов.

– Емкость – количество регулярно архивируемых данных. Справится ли оборудование с нагрузкой в отведенное время?

– Надежность аппаратных средств и носителей. Можете ли вы пожертвовать надежностью ради экономии или скорости?

– Расширяемость решения. Удовлетворяет ли ваше решение потребностям роста организации?

– Скорость архивации и восстановления. Можете ли вы пожертвовать скоростью ради снижения стоимости?

– Цена архивации. Приемлема ли она для вашего бюджета?

Типовые решения архивации

Итак, на план архивации влияют емкость, надежность, расширяемость, скорость и цена. Определив, какие из этих факторов наиболее важны для вашей организации, вы примете подходящее решение. Вот некоторые общие рекомендации:

– Ленточные накопители — самые распространенные устройства архивации. Данные хранятся на кассетах с магнитной лентой. Лента относительно недорога, но не особенно надежна: она может помяться или растянуться, с течением времени — размагнититься и перестать считываться. Средняя емкость кассет с лентой варьируется от единиц до десятков Гбайт. По сравнению с другими решениями ленточные накопители довольно медленны. Их достоинство – невысокая цена.

– Накопители на цифровой ленте (digital audio tape, DAT) – пришли на смену традиционным ленточным накопителям. Существует несколько форматов DAT, их емкости составляют 35 и 260 Гбайт.

– Ленточная библиотека с автозагрузкой – устройство для создания расширенных архивных томов на нескольких лентах, которых хватает для нужд всего предприятия. Ленты набора в процессе архивации или восстановления данных автоматически меняются. В большинстве таких библиотек применяются DAT-ленты. Их главный минус – высокая цена.

– Магнитооптические накопители с автозагрузкой подобны ленточным библиотекам, только вместо лент в них используются магнитооптические диски. Цена также очень высока.

– Съемные диски, например Iomega Jazz емкостью 1-2 Гбайт обладают хорошей скоростью и удобны в работе, но стоят дороже ленточных или DAT-накопителей.

– Дисковые накопители обеспечивают наивысшую скорость при архивации и восстановлении файлов. Если при архивации на ленту вам потребуются часы, то дисковый накопитель позволяет завершить процесс за несколько минут. К недостаткам дисковых накопителей следует отнести относительно высокую цену на единицу объема.

2.2. Порядок выполнения практической работы

2.2.1. Запустить виртуальную машину.

2.2.2. Создать задания на выполнения архивации данных

– Создать на диске **C:** папку с именами студентов, выполняющих работу и номером группы (например, **C:\362-2_Ivanov_Petrov**), в которой создать каталоги **library**, **backup** и **restore**;

– В папке **library** создать 3 текстовых файла с наименованиями **book1.txt**, **book2.txt** и **book3.txt**.

– Запустить утилиту резервного копирования **ntbackup**.

Эту утилиту можно запустить из Главного меню системы (кнопка **"Пуск" – "Все программы" – "Стандартные" – "Служебные" – "Архивация данных"**), а можно запустить более быстро из командной строки (кнопка **"Пуск" – "Выполнить" – "ntbackup" – кнопка "ОК"**). При первом запуске утилиты убрать галочку у поля "Всегда запускать в режиме мастера" и нажать ссылку "**Расширенный режим**".

– Запустить "Мастер архивации" (на закладке "Добро пожаловать" нажать кнопку "Мастер архивации".

– После запуска мастера нажмем кнопку "Далее" и выберем, что нам нужно архивировать, в данном примере – "Архивировать выбранные файлы, диски или сетевые данные"

– Выберем для архивирования папку **library**.

– Выберем место для создания резервной копии, создадим файл с именем **library**, этому файлу автоматически будет назначено расширение ".**bkf**".

– На данном этапе нажмем кнопку "**Готово**".

– Проверяем полученный результат (на вкладке **Восстановление и управление носителем**).

2.2.3. Изучение использования различных методов резервирования.

– Вносим изменения в файл *book1.txt* и *book2.txt*, у файла *book1.txt* убираем атрибут **"Файл готов для архивирования"**, а *book3.txt* – удаляем.

– Запускаем снова мастер архивации, но вместо кнопки "Готово" нажимаем кнопку "**Дополнительно**", чтобы задать дополнительные параметры и выбираем тип архивации **"Добавочный"** и жмем кнопку **"Далее"**. Далее все пункты по умолчанию, но при этом не забывайте запоминать, что Вы делаете. Проверяем полученный результат. **Почему он такой?**

2.2.4. Восстановление файлов.

Восстановите файл *book3.txt*. Для этого выполните следующие действия:

– Запустим утилиту резервного копирования **ntbackup**.

– Перейдем на закладку "**Восстановление и управление носителем**".

– После появления в списке архивных файлов нужного архива раскроем этот архив и выберем файлы для восстановления из резервной копии. При этом мы можем восстановить файлы в то место, где они были ранее ("**Исходное размещение**") или выбрать иной путь для их сохранения ("**Альтернативное размещение**"). Выберите папку **restore**.

– После определения всех параметров восстановления нажмем кнопку "**Восстановить**", утерянные данные будут восстановлены.

2.2.5. Использование дополнительных возможностей архивации.

Для выполнения данного задания необходимо сначала задать пароль пользователю, от имени которого идет работа. Для этого сделайте следующее. Нажмите **Пуск – Панель управления – Учетные записи пользователей**. Выберите нужного пользователя, щелкнув на его имени левой кнопкой мыши. Затем нажмите "**Задать пароль**".

Создайте задания на выполнение архивации данных для папки **library**, используя выбор дополнительных возможностей:

– Выбираем тип архивирования (выберем "Обычный").

– Ничего не меняем на странице "Способы архивации".

– На странице «Параметры архивации» можно выбрать замену существующих архивов или добавление архива (если файл с архивной копией уже существует).

– На странице "Когда архивировать" задайте расписание для автоматического создания резервной копии – выберите вариант "Позднее" и задайте расписание архивирования, чтобы архивирование происходило ежедневно. Время начала установите, исходя из текущего времени системы + пять минут.

– Нажмите далее. Система запросит имя и пароль пользователя, с чьими полномочиями будет выполняться задание архивирования. В серверных операционных системах рекомендуется для выполнения заданий резервного копирования создавать специальные учетные записи, обладающие достаточными правами (как минимум члены группы "Операторы архива").

– Нажмем кнопку "Готово", задание будет создано, и оно появится в списке "Назначенных заданий". Теперь оно будет выполняться регулярно в соответствии с расписанием.

– Завершите сеанс администратора, ожидайте до завершения задания. После проверьте результат.

2.2.6. Архивирование и восстановление состояния системы.

Большую часть работ по резервному копированию составляют задания на копирование бизнес-информации. Но имеется также возможность создания резервных копий для восстановления функционирования самой операционной системы.

Для создания резервной копии состояния системы необходимо в утилите резервного копирования *ntbackup* при создании задания на архивирования отметить галочкой пункт "**Архивировать выбранные файлы, диски или сетевые данные**", а затем выбрать подпункт "**System State**" пункта **"Мой компьютер"** либо выбрать пункт **"Архивировать только данные состояния системы"**.

При этом будут архивироваться следующие данные:

– системный реестр;

– база данных зарегистрированных классов объектов (*Class Registration*);

– системные загрузочные файлы;

– база данных служб сертификатов (только на серверах, на которых установлена служба сертификатов);

– база данных *Active Directory* и папка *SYSVOL* (на серверах – контроллерах доменов).

Для архивирования состояния системы, а также для последующего восстановления, обязательно нужны права администратора данного компьютера. Восстановление *Active Directory* необходимо выполнять только при загрузке системы в режиме восстановления служб каталогов (запуск меню выбора режимов загрузки операционной системы Windows Server 2003 осуществляется в начальный момент загрузки нажатием клавиши F8).

Сетевой администратор (ИТ-руководство компании) должны уделять вопросам резервного копирования самое пристальное внимание, т.к. от грамотно построенной и надежно работающей системы резервного копирования зависит, насколько быстро и удачно будет произведено восстановление информации, поврежденной в результате действий персонала, аппаратных сбоев, вирусных атак и прочих инцидентов.

3. Работа с реестром ОС Windows XP

Цель работы: Изучить возможности оптимизации ОС Windows XP с помощью реестра.

3.1. Краткие теоретические сведения

Реестр является основополагающим элементом ОС Windows XP. Он содержит конфигурационные данные, которые позволяют ОС корректно функционировать. При этом конфигурационные данные организуются в Реестре особым образом, а его организационная структура не может быть воспроизведена в каком-либо другом механизме или файле ОС, кроме самого Реестра. Все декларированные, а также не декларированные возможности ОС, в том числе, те из них, которые не могут быть настроены с использованием графического пользовательского интерфейса (GUI), могут быть конфигурированы посредством Реестра. Любое запускаемое в системе приложение не может быть выполнено без обращения к Реестру, поскольку именно там находятся все его параметры.

Физически Реестр ОС Windows XP представляет собой иерархическую базу данных, в которой содержатся важные сведения о системном оборудовании, установленных программах и их параметрах, а также профилях каждой из учетных записей пользователей компьютера. Все приложения и сама ОС постоянно обращаются к этим сведениям для своей работы. Эта база данных хранится в системных файлах ОС, в частности, system.dat и ntuser.dat. Основными элементами структуры Реестра ОС являются ключи. Каждый ключ может иметь набор параметров, каждому из которых соответствует определенное значение, а также подключи – подчиненные ключи более низкого уровня. По отношению к друг другу ключи и подключи организуются в системном Реестре в соответствии с отношением вида "предок-потомок". Иерархическая структура Реестра ОС представляет собой дерево ключей, организованное в виде кустов или ульев (каждый из которых является двоичным файлом, называемым файлом куста), напоминающей структуру файлов и папок файловой системы (ФС). Корневой ключ (вершина дерева) и подключи по аналогии с ФС можно считать папками, а параметры Реестра – файлами, соответственно. В качестве кустов корневого ключа **HKEY_LOCAL_MACHINE (HKLM)** и соответствующих им файлов кустов можно привести следующий пример (табл. 3.1). Каждый из файлов кустов **HKLM** имеет свой

системный путь. В частности, файлы кустов **HKLM\SOFTWARE** и **HKLM\SYSTEM** находятся в системном каталоге %SYSTEMROOT%\System32\config.

Таблица 3.1. Файлы кустов корневого ключа **HKLM**

№ п/п.	Куст	Файл куста
1.	**HKLM\SAM**	Sam.log
2.	**HKLM\SECURITY**	Security.log
3.	**HKLM\SOFTWARE**	Software.log, Software.sav
4.	**HKLM\SYSTEM**	System.log, System.sav

Следует отметить, что в таблице отображены не все кусты **HKLM**, а лишь те из них, которые являются постоянными Реестра ОС. В дополнение имеются два временных куста **HKLM,** образующиеся при старте системы. Куст **HKLM\SYSTEM** корневого ключа **HKLM** является основным системным кустом, так как в него входит подключ **\CurrentControlSet\Control**, содержащий параметры, которые компонент ядра ОС, называемый "Менеджер конфигурации" (Configuration Manager), использует при инициализации Реестра. При этом значение **hivelist** подключа **\CurrentControlSet\Control** используется системой при поиске остальных ее файлов куста. В рассмотренном примере одним из ключей системного Реестра был назван корневой ключ **HKEY_LOCAL_MACHINE**. Но в отличие от ФС, в которой имеется только один корневой каталог, Реестр ОС имеет несколько корневых ключей высшего уровня, каждый из которых определяет некоторую категорию данных, хранимых в Реестре. Полный список корневых ключей, а также их краткое описание представлены ниже (табл. 3.2). Некоторые ключи и соответствующие им кусты являются временными. К их числу можно отнести корневые ключи **HKU**, **HKDD** и некоторые **HKLM** с соответствующими кустами **HKLM\HARDWARE** и **HKLM\SYSTEM\Clone**. ОС создает их каждый раз при загрузке и хранит в оперативной памяти до момента завершения сеанса работы.

Таблица 3.2. Корневые ключи Реестра ОС Windows XP

№ п/п.	Ключ	Описание
1.	**HKCR**	**HKEY_CLASSES_ROOT.** Подключи этого корневого ключа содержат основную информацию о типах файлов, зарегистрированных в системе. Названия подключей совпадают с соответствующими расширениями файлов. Корневому ключу **HKCR** подчиняются описания различных программных средств обработки этих файлов, а также сведения обо всех категориях зарегистрированных объектов.
2.	**HKCU**	**HKEY_CURRENT_USER.** Эта категория содержит описание параметров, меняющихся в зависимости от профиля пользователя, в данный момент работающего в системе. Изменения, относящиеся к текущему пользователю, следует всегда вносить именно сюда, так как они автоматически копируются для длительного хранения при завершений работы компьютера и восстанавливаются в ходе начальной загрузки ОС.
3.	**HKLM**	**HKEY_LOCAL_MACHINE.** Этот раздел отвечает за информацию об аппаратных компонентах компьютера и средствах, обеспечивающих их работу. Здесь также хранится общая информация об установленном программном обеспечении.
4.	**HKU**	**HKEY_USERS.** Этот раздел содержит подключи, соответствующие всем пользователям, зарегистрированным на данном компьютере. Когда один из пользователей начинает работу в системе, ОС автоматически копирует соответствующий ключ **HKU** в раздел **HKCU**. При завершении сеанса пользователя данные копируются обратно.

Продолжение таблицы 3.2

5.	**HKCC**	**HKEY_CURRENT_CONFIG.** В этом разделе дублируется информация (текущий набор конфигурационных параметров аппаратуры) о некоторых устройствах компьютера, в первую очередь о видеоадаптере и принтере.
6.	**HKDD**	**HKEY_DYN_DATA.** Этот раздел содержит текущую информацию о работе компьютера, обычно обновляемую в режиме реального времени. Основные подключи содержат данные об устройствах, работающих в настоящее время, а также сведения о текущем значении статистических параметров. Отобразить эти данные позволяет служебный модуль **«Системный монитор»**.

Возвращаясь к вопросу о параметрах ключей и их значениях, следует сказать, что каждый ключ содержит как минимум одно значение какого-либо параметра. Как у любого файла в ФС, у параметра значения имеется имя, в то время как расширение файла похоже на его тип. Данные значения по аналогии с ФС похожи на конкретное содержимое файла. Из сказанного следует, что каждый ключ или подключ имеет одно или более значений, в свою очередь, каждое из которых характеризуется именем соответствующего параметра, типом и хранимыми в нем данными. Имя параметра значения (или просто имя значения) представляет собой строку, содержащую до 512 символов в кодировке ANSI (или 256 символов в кодировке Unicode), за исключением символов, зарегистрированных для имен ОС Windows XP. Всего для значений предусмотрено пятнадцать различных типов, три из которых: **REG_BINARY**, **REG_DWORD** и **REG_SZ** являются основными и описывают большинство всех значений в Реестре ОС. Двоичные данные значений типа **REG_BINARY**, записанные в шестнадцатеричном виде, представляют собой строку байтов произвольной длины. Их обычно применяют в том случае, когда параметр должен хранить набор данных определенной структуры. Значения типа **REG_DWORD** имеют длину данных в два машинных слова (четыре байта) и записываются в десятичной или шестнадцатеричной форме. Многие значения в Реестре принадлежат этому типу и используются в качестве логических флагов: 0 или 1, да или нет, истина или ложь; иногда значения этого типа встречаются в миллисекундах (1000 равно 1 секунде), описывающих время. Наконец, значение типа **REG_SZ** представляет собой текст постоянной длины в виде строки символов,

например, "Microsoft Windows XP". Каждая строка заканчивается символом **null**. Приложения не преобразуют значения этого типа, а транслируют и отображают их "как есть".

В практической работе предполагается изучение основных возможностей редактирования Реестра ОС Windows XP, изменения значений параметров его ключей, а также создания резервных копий с целью его дальнейшего восстановления.

3.2. Подготовка к выполнению практической работы

Перед началом выполнения практической работы в среде ОС Windows XP необходимо осуществить следующее:

1) загрузить ОС Windows XP и активировать справочное меню **(Пуск | Справка и поддержка)**;

2) ознакомиться с описанием Реестра и возможностями его применения в ОС Windows XP;

3) ознакомиться с описанием и возможностями служебного программного средства **«Редактор Реестра» (Regedit)**, изучив справочный материал по данному приложению, находящийся в системном каталоге **C:\Windows\Help** в одноименном файле с расширением **.chm**;

4) воспользовавшись ключом **/?**, ознакомиться с описанием и возможностями консольной утилиты **Reg.exe** для работы с Реестром ОС, доступной из командной строки.

3.3. Порядок выполнения практической работы

Практическая работа выполняется последовательно в соответствии с определенным порядком и включает в себя два учебных задания.

Практическая работа подразумевает изучение возможностей конфигурирования ОС Windows XP посредством специальных настроек реестра, твиков и скриптов на его основе, направленных на оптимизацию работы системы.

Оптимизация ОС посредством реестра является высшим пилотажем с точки зрения IT-профессионалов и опытных пользователей, поскольку требует тщательного изучения самого реестра, инструментов для его редактирования, достаточно обширных знаний операционных систем, принципов их

функционирования, а также достаточного опыта настройки ОС стандартными программными средствами и утилитами сторонних производителей.

Оптимизация как процесс предполагает настройку и конфигурирование ОС таким образом, чтобы получить стабильно работающую систему, с одной стороны, но при этом достаточно быструю и оптимально расходующую системные ресурсы, с другой стороны. Оптимизация ОС с использованием реестра может быть осуществлена вручную, когда IT-профессионал самостоятельно вводит конкретные параметры и значения в реестр для достижения заранее определенного результата, отчетливо зная при этом, что именно он изменяет и для чего он это делает. При этом он может облегчить ввод этих значений, написав сценарий или скрипт с целым рядом необходимых параметров и применив его к системе одним из способов изученных ранее. Другой путь, назовем его автоматизированный, скорее подходит для тех лиц, кто не обладает значительными знаниями архитектуры ОС и принципов ее функционирования, а именно для рядовых пользователей и тех, кто только начинает приобретать знания в этой сфере. Этот путь заключается в том, чтобы использовать для настройки ОС, так называемые, твики реестра ОС и написанные профессиональными программистами скрипты. Отчасти, это может гарантировать некоторую степень безопасного изменения настроек системы. Наконец, полностью автоматизированная настройка ОС возможна только в том случае, если твики реестра или скрипты управляют автоматически процессом распространения настроек по сети и их применением в системе. Этот путь требует для своего осуществления не только достаточных знаний архитектуры и реестра ОС, но дополнительно, как минимум, одного языка программирования, а также способов передачи данных по сетям. Как правило, багаж знаний и опыта, необходимый для его реализации, может быть достигнут через несколько лет практической работы в области компьютерных технологий и программирования в частности. Непосредственного написания скриптов на одном из языков программирования в настоящем практикуме не предполагается. Это вопрос отдельной дисциплины. Упоминаемое в рамках настоящей практической работы, понятие "твик реестра" (от англ. tweak – настройка) соответствует некоторой настройке программного обеспечения (ПО) или операционной системы, хранящейся в системном реестре. Твики позволяют автоматизировать настройку ПО. К тому же, многие параметры легче настроить при помощи твика реестра ОС, чем посредством GUI. Твик реестра ОС представляет собой текстовый Reg-файл, который может быть создан в любом

текстовом редакторе и сохранен в кодировке ANSI или Unicode. В качестве классического примера ниже приводится содержимое Reg-файла, отключающего меню недавних документов. При этом обратите внимание на принцип построения и синтаксис данного файла, который использует следующие системные символы:

; – для справочной информации, которая является неисполняемой при внесении данных в реестр ОС,

[и **]** – для указания ключа реестра, в который будет вноситься его новое значение,

" и **"** – для непосредственной идентификации параметра, подлежащего изменению.

Файл твика реестра ОС Windows XP (Reg-файл) имеет стандартный вид:

```
Windows Registry Editor Version 5.00
;Отключить меню недавних документов
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]
"NoRecentDocsMenu"=hex:01,00,00,00
```

Импорт приведенного твика реестра и его интеграция в ОС осуществляется одним из способов, изученных ранее на практическом задании. Глобально все твики и настройки реестра ОС можно разделить на несколько категорий, по их принадлежности к корневым ключам, в частности, **HKLM** и **HKCU**. По результатам, получаемым при применении настроек в системе, они подразделяются на: настройки пользователей и настройки интерфейса ОС. Отдельно можно определить настройки оптимизации ОС и конфигурирования системных служб. В рамках настоящей практической работы последнюю категорию настроек предполагается рассмотреть более подробно.

Задание №3.1. Запуск редактора реестра и первое знакомство с реестром Windows XP. Экспорт и импорт реестра.

1. Откройте "**Редактор Реестра**", одновременно нажав клавиши **"WIN"** (на ней изображен флаг-логотип MS Windows) **+ "R"**, введя в появившемся окне "**Выполнить**" строку **Regedit** и нажав **Enter** для подтверждения ввода.

Альтернативный способ запуска приложения состоит в следующем:

- нажмите **Пуск | Выполнить**,

– наберите в появившемся окне **Regedit.exe** (или просто **Regedit**),

– нажмите **Enter** для ввода.

2. В появившемся окне "**Редактора Реестра"** обратите внимание на то, что с левой стороны окна расположена панель ключей, а с правой стороны – панель значений. Панель ключей отображает корневые ключи и подключи Реестра. Щелкая манипулятором мышь по корневым ключам Реестра, отобразите слева его иерархию. Панель значений справа демонстрирует настройки, содержащиеся в каждом из подключей. Щелкните по одному из них на панели ключей и найдите его значения на панели значений.

Термин "Ветвь" относится к ключу и всем его подключам. Разворачивать и сворачивать ключи и подключи также можно, щелкая манипулятором мышь на значках узла с соответствующим символом "**+"** или **"–"**. На панели ключей выберите ветвь Реестра **HKLM\System\Setup** и разверните ее, щелкнув на узле с символом "**+".** На панели значений найдите параметр с именем **SystemPartition** и определите строку данных этого значения.

3. Самостоятельно выберите в Реестре ОС какой-либо ключ (с соответствующими подключами), содержащий одновременно значения с основными системными типами **REG_BINARY**, **REG_DWORD** и **REG_SZ**. Обратите внимание на имеющуюся в редакторе возможность представления данных выбранного значения в двоичном виде (команда "**Вывод двоичных данных"** в меню "**Вид"**).

4. Экспорт Реестра ОС или его части это одна из тех вещей, которые достаточно часто приходится делать системным администраторам и опытным пользователям. По сути, экспорт представляет собой копирование данных в другой файл. По отношению к Реестру, этот файл имеет расширение **.reg**. Экспорт настроек в **Reg**-файл имеет практическую ценность. Прежде всего, это великолепный способ создать резервную копию системных настроек на случай их экстренного восстановления при необходимости. Это также хороший способ передавать настройки другим пользователям на другие компьютеры сети. Имея несколько **Reg**-файлов с различными настройками системы, возможно импортировать их одним двойным щелчком мышью. Для экспорта ветвей реестра выполните следующие инструкции:

– щелкните мышью на ключе, находящемся в вершине ветви, выбранной самостоятельно, которую необходимо экспортировать,

– в меню "**Файл**" выберите пункт "**Экспорт**", чтобы вывести на экран диалоговое окно **"Экспорт файла Реестра"**,

– в поле "**Имя файла**" введите имя файла для экспорта,

– выберите диапазон экспорта: чтобы создать копию всего реестра, щелкните на **"Весь реестр"**, чтобы создать копию выделенной ветви, щелкните на "**Выбранная ветвь**",

– в выпадающем списке **"Тип файла"** выберите тип файла для экспорта: "Файлы Реестра *.reg", "Файлы кустов Реестра *.*", "Текстовые файлы *.txt" или "Файлы Реестра Win9x/NT4 *.reg",

– экспортируйте ветвь, мышью щелкнув на кнопке "**Сохранить**".

Последовательность вышеописанных действий фактически представляет собой один из способов создания резервной копии Реестра ОС. Сохранение Реестра перед его редактированием является принципиальным, поскольку обеспечивает дополнительный шанс на его восстановление в случае выхода системы из строя посредством непродуманных действий пользователя. Обратная процедура импорта Реестра практически ни чем не отличается от простого открытия **Reg**-файла. Для этого необходимо щелкнуть мышью на пункте "**Импорт**" в меню "**Файл**", далее в выпадающем списке "**Тип файла**" выбрать тип файла, который предполагается импортировать, а затем в поле "**Имя файла**" ввести полный путь **Reg**-файла и подтвердить операцию, щелкнув по кнопке **"Открыть"**.

Альтернативный способ импорта Реестра ОС заключается в следующем:

– в "**Проводнике**" дважды щелкните мышью на **Reg**-файле**,** чтобы внести его содержимое в Реестр,

– подтвердите внесение настроек в Реестр, щелкнув мышью по кнопке **"Да"**, после чего должно последовать сообщение об успешном завершении операции.

Внимание! Файлы Реестра ОС Windows XP представляют собой пятую версию **Reg**-файлов. Другие ОС семейства Windows имеют другие версии **Reg**-файлов. Поэтому не импортируйте **Reg**-файл, созданный в одной версии ОС Windows, в другую версию этой ОС. Это может привести к неработоспособности последней.

Задание №3.2. Конфигурирование контекстного меню служебного программного средства "Мой компьютер" ОС Windows XP посредством применения твика реестра.

Первая группа системных настроек имеет отношение к контекстному меню служебного приложения "Мой компьютер", возникающего при одиночном клике правой кнопкой манипулятора мышь на соответствующей иконке в меню **"Пуск"**. Сущность данных настроек заключается в том, что при их применении контекстное меню приложения **"Мой компьютер"** приобретает несколько иной вид, а именно в нем становятся доступными некоторые системные программы (например, **"Проводник"**) и функции. Польза такого новшества очевидна, поскольку фактически в один клик становятся доступными все необходимые системному администратору инструменты. Это существенно экономит время работы IT-профессионала или опытного пользователя. Ниже приводится список настроек реестра ОС, преобразующих контекстное меню штатного приложения **"Мой компьютер"** как показано на рис. 5.1. Данные системные настройки могут быть применены в ОС как по отдельности, так и в составе программного твика реестра.

1. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Администрирование"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\1]

@="Администрирование"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\1\command]

@="control admintools"

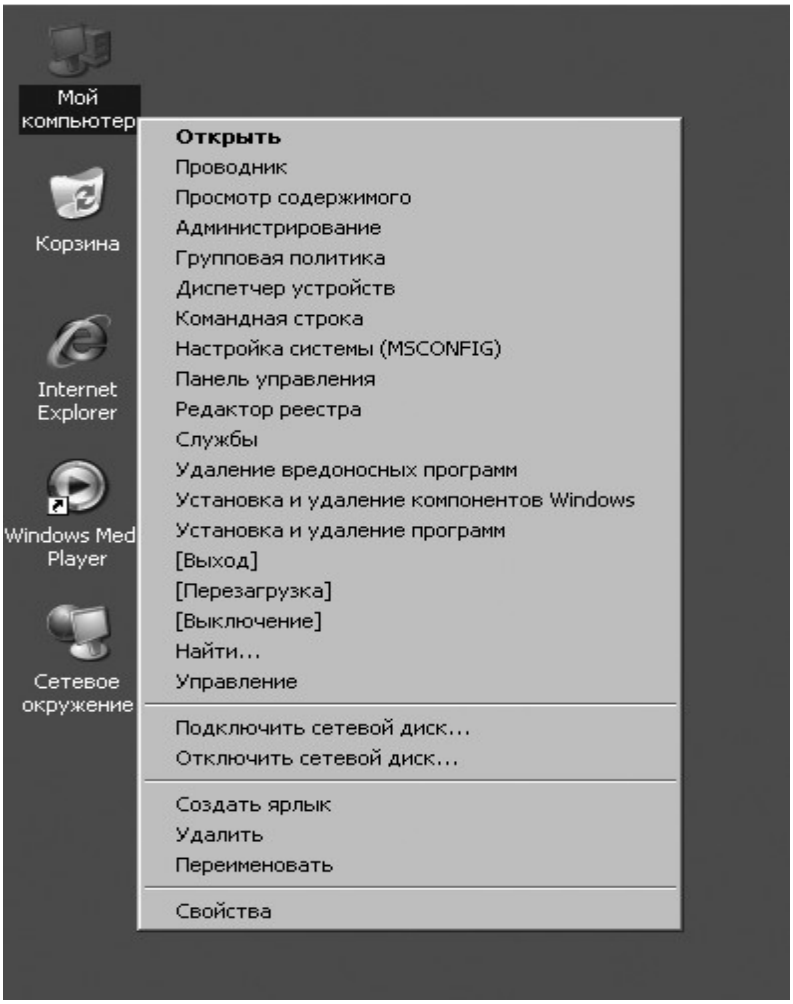


Рисунок 3.1 – Внешний вид контекстного меню **"Мой компьютер"** после применения настроек в системном реестре

2. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Командная строка"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\22]

@="Командная строка"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\22\command]

@="cmd.exe"

3. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Настройка системы"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\3]

@="Настройка системы (MSCONFIG)"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\3\command]

@="msconfig.exe /s"

4. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Панель управления"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\4]

@="Панель управления"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\4\command]

@="rundll32.exe shell32.dll,Control_RunDLL"

5. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Редактор реестра"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\44]

@="Редактор реестра"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\44\command]

@="Regedit.exe"

6. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Удаление вредоносных программ"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\55]

@="Удаление вредоносных программ"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\55\command]

@="mrt.exe"

7. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Установка и удаление компонентов Windows"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\6]

@="Установка и удаление компонентов Windows"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\6\command]

@="rundll32 shell32,Control_RunDLL appwiz.cpl,,2"

8. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Установка и удаление программ"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\66]

@="Установка и удаление программ"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\66\command]

@="control appwiz.cpl"

9. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Выход"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\7]

@="[Выход]"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\7\command]

@="shutdown -l -f -t 0"

10. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Перезагрузка"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\77]

@="[Перезагрузка]"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\77\command]

@="shutdown -r -f -t 0"

11. Настройка добавляет в контекстное меню приложения **"Мой компьютер"** команду **"Выключение"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\8]

@="[Выключение]"

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\8\command]

@="shutdown -s -f -t 0"

Для создания твика реестра ОС с целью конфигурирования контекстного меню приложения **"Мой компьютер"**, выполните следующие действия:

- из перечисленных выше настроек реестра ОС выберите те (в количестве не менее 5 штук), которые наиболее подходят для Ваших персональных целей,
- самостоятельно создайте текстовый **Reg**-файл с именем, включающим **номер группы и фамилии студентов**, выполняющих данную работу.
- откройте созданный твик-файл и напечатайте первой его строкой следующее **Windows Registry Editor Version 5.00**,

- отредактируйте твик-файл, скопировав в него выбранные ранее настройки реестра ОС,
- сохраните созданный твик реестра ОС.

Конфигурирование контекстного меню приложения **"Мой компьютер"** в ОС Windows XP осуществите следующим образом:

- выполните экспорт реестра одним из изученных способов.
- примените созданный Вами твик реестра в системе,
- выйдите из сеанса пользователя и снова войдите в систему, чтобы параметры вступили в силу,
- сделайте вывод о проделанной работе.

Задание №3.3. Конфигурирование ОС Windows XP с целью оптимизации ее работы и увеличения быстродействия.

Вторая группа системных настроек предназначена для оптимизации и увеличения быстродействия ОС Windows XP. Однако оптимизация системы не ограничивается применением только данного набора настроек; существует ряд других системных твиков, позволяющих оптимизировать ее работу. Ниже представлен список части настроек реестра ОС, наиболее интересных с точки зрения увеличения производительности некоторых подсистем. Как и в предыдущем случае, каждая из них может быть использована в виде отдельного твика, а также при непосредственном редактировании реестра ОС и внесении значений указанных параметров вручную.

1. Настройка позволяет оптимизировать расположение загрузочных файлов на жестком диске для ускорения их загрузки:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Dfrg\BootOptimizeFunction]
"Enable"="Y"
```

2. Настройка отключает сообщения о второстепенных ошибках в системе, но при этом уведомление о критических системных ошибках остается:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\PCHealth\ErrorReporting]
"AllOrNone"=dword:00000000
"IncludeMicrosoftApps"=dword:00000000
"IncludeWindowsApps"=dword:00000001
"IncludeKernelFaults"=dword:00000001
"DoReport"=dword:00000000
"ShowUI"=dword:00000000

3. Настройка отключает уведомления Центра обеспечения безопасности ОС Windows XP:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center]
;Отключить предупреждения Брэндмауэра
"FirewallDisableNotify"=dword:00000001
;Отключить предупреждения службы Автоматического обновления
"UpdatesDisableNotify"=dword:00000001
;Отключить предупреждения системы Антивирусной защиты "AntiVirusDisableNotify"=dword:00000001

4. Настойка обеспечивает ускорение ОС при перезагрузке:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"EnableQuickReboot"="1"

5. Настройка позволяет уменьшить использование доступного места на диске, отведенного для **"Корзины",** до 3% от общего пространства вместо 10%, отводимых системой по умолчанию:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\BitBucket]
"Percent"=dword:00000003

6. Настройка позволяет ускорить открытие служебного приложения **"Мой компьютер"**:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer]

"NoRemoteRecursiveEvents"=dword:00000001

7. Настройка ускоряет процесс выключения компьютера:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control]

"WaitToKillServiceTimeout"="2000"

8. Настройка позволяет зарезервировать оптимальный размер для главной таблицы размещения файлов MFT:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem]

"NtfsMftZoneReservation"=dword:00000003

9. Настройка осуществляет ускорение работы оптического привода:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\CDFS]

"Prefetch"=dword:00004000

"PrefetchTail"=dword:00004000

"CacheSize"=hex:ff,ff,00,00

10. Настройка осуществляет исправление неполадок при отображении символов кириллицы в приложениях:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage]

"1250"="c_1251.nls"

"1251"="c_1251.nls"

"1252"="c_1251.nls"

"1253"="c_1251.nls"

11. Настройка позволяет осуществить отображение подробной системной информации в служебном модуле **"Диспетчер устройств"**:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Environment]

"DEVMGR_SHOW_DETAILS"=dword:00000001

12. Настройка позволяет осуществить очистку файла подкачки при выключении компьютера:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]

"ClearPageFileAtShutdown"=dword:00000001

13. Настройка позволяет увеличить производительность ОС в целом:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management]
"DisablePagingExecutive"=dword:00000001

14. Настройка позволяет ускорить загрузку ОС:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\MemoryManagement\PrefetchParameters]
"EnablePrefetcher"=dword:00000003

15. Настройка укоряет загрузку веб-страниц:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\ServiceProvider]
"DnsPriority"=dword:00000001
"HostsPriority"=dword:00000001
"LocalPriority"=dword:00000001
"NetbtPriority"=dword:00000001

16. Настройка позволяет отключить проверку дисков при загрузке:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
"AutoChkTimeOut"=dword:0000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager]
"BootExecute"=hex(7):61,00,75,00,74,00,6f,00,63,00,68,00,65,00,63,00,6b,00,20,\
00,61,00,75,00,74,00,6f,00,63,00,68,00,6b,00,20,00,2a,00,00,00,00,00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon]
"SFCScan"=dword:00000000

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\MyComputer\cleanuppath]

@=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,\
00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,63,00,6c,00,\
65,00,61,00,6e,00,6d,00,67,00,72,00,2e,00,65,00,78,00,65,00,20,00,2f,00,44,\
00,20,00,25,00,63,00,00,00

17. Настройка позволяет отключить автозапуск для всех типов оптических приводов и устройств в системе:

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer]
"NoDriveTypeAutoRun"=dword:000000ff

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Cdrom]
"AutoRun"=dword:00000000

Для изучения результатов применения указанного комплекта системных настроек реестра ОС выполните следующее.

- выполните экспорт реестра одним из изученных способов.
- последовательно примените к системе не менее 5 выбранных самостоятельно настроек реестра ОС без использования твиков,
- выйдите из сеанса пользователя и снова войдите в систему, чтобы параметры вступили в силу, при этом каждый раз наблюдая за стабильностью работы ОС,
- сделайте вывод о проделанной работе.

Изученные в настоящей практической работе возможности обеспечивают системного администратора базовым инструментарием тонкой настройки ОС Windows XP. Набор описанных настроек и твиков системного реестра способствует оптимизации и ускорению работы ОС. Однако, конфигурирование системы посредством указанных настроек это лишь малая часть всех работ, направленных на обеспечение оптимальной и эффективной работы системы. Среди прочего, к числу подобного рода мероприятий следует отнести работы по настройке и оптимизации системных служб ОС Windows XP, в частности, за счет их включения или отключения посредством системного реестра.

В заключение следует отметить, что для более подробного изучения рассмотренных в практической работе вопросов целесообразно обратится к первоисточнику, книге "Реестр Microsoft Windows XP" автора Джерри Хонейкатт, который является признанным специалистом в этой области. Кроме того, различные возможности настройки системы, твики реестра ОС, скрипты для их системного применения в достаточном количестве можно найти в глобальной сети Интернет. Одним из сетевых ресурсов является специализированный сайт **www.OSzone.net**, в основном посвященный вопросам, связанным с операционными системами семейства Windows. На этом сайте опубликованы различные инструкции и рекомендации по конфигурированию ОС, в большом количестве приведены системные настройки и твики, а также специализированные обзоры и статьи по смежным тематикам.

4. Работа с Реестром ОС Windows XP. Продолжение

Цель работы: Изучить сущность Реестра, его структуру и возможности оптимизации ОС Windows XP с его помощью.

4.1. Краткие теоретические сведения

Реестр является основополагающим элементом ОС Windows XP. Он содержит конфигурационные данные, которые позволяют ОС корректно функционировать. При этом конфигурационные данные организуются в Реестре особым образом, а его организационная структура не может быть воспроизведена в каком-либо другом механизме или файле ОС, кроме самого Реестра. Все декларированные, а также не декларированные возможности ОС, в том числе, те из них, которые не могут быть настроены с использованием графического пользовательского интерфейса (GUI), могут быть конфигурированы посредством Реестра. Любое запускаемое в системе приложение не может быть выполнено без обращения к Реестру, поскольку именно там находятся все его параметры.

Физически Реестр ОС Windows XP представляет собой иерархическую базу данных, в которой содержатся важные сведения о системном оборудовании, установленных программах и их параметрах, а также профилях каждой из учетных записей пользователей компьютера. Все приложения и сама ОС постоянно обращаются к этим сведениям для своей работы. Эта база данных хранится в системных файлах ОС, в частности, system.dat и ntuser.dat. Основными элементами структуры Реестра ОС являются ключи. Каждый ключ может иметь набор параметров, каждому из которых соответствует определенное значение, а также подключи – подчиненные ключи более низкого уровня. По отношению к друг другу ключи и подключи организуются в системном Реестре в соответствии с отношением вида "предок-потомок". Иерархическая структура Реестра ОС представляет собой дерево ключей, организованное в виде кустов или ульев (каждый из которых является двоичным файлом, называемым файлом куста), напоминающей структуру файлов и папок файловой системы (ФС). Корневой ключ (вершина дерева) и подключи по аналогии с ФС можно считать папками, а параметры Реестра – файлами, соответственно. В качестве кустов корневого ключа **HKEY_LOCAL_MACHINE (HKLM)** и соответствующих им файлов кустов можно привести следующий пример (табл. 4.1). Каждый из файлов кустов **HKLM** имеет свой

системный путь. В частности, файлы кустов **HKLM\SOFTWARE** и **HKLM\SYSTEM** находятся в системном каталоге %SYSTEMROOT%\System32\config.

Таблица 4.1. Файлы кустов корневого ключа **HKLM**

№ п/п.	Куст	Файл куста
1.	**HKLM\SAM**	Sam.log
2.	**HKLM\SECURITY**	Security.log
3.	**HKLM\SOFTWARE**	Software.log, Software.sav
4.	**HKLM\SYSTEM**	System.log, System.sav

Следует отметить, что в таблице отображены не все кусты **HKLM**, а лишь те из них, которые являются постоянными Реестра ОС. В дополнение имеются два временных куста **HKLM,** образующиеся при старте системы. Куст **HKLM\SYSTEM** корневого ключа **HKLM** является основным системным кустом, так как в него входит подключ **\CurrentControlSet\Control**, содержащий параметры, которые компонент ядра ОС, называемый "Менеджер конфигурации" (Configuration Manager), использует при инициализации Реестра. При этом значение **hivelist** подключа **\CurrentControlSet\Control** используется системой при поиске остальных ее файлов куста. В рассмотренном примере одним из ключей системного Реестра был назван корневой ключ **HKEY_LOCAL_MACHINE**. Но в отличие от ФС, в которой имеется только один корневой каталог, Реестр ОС имеет несколько корневых ключей высшего уровня, каждый из которых определяет некоторую категорию данных, хранимых в Реестре. Полный список корневых ключей, а также их краткое описание представлены ниже (табл. 4.2). Некоторые ключи и соответствующие им кусты являются временными. К их числу можно отнести корневые ключи **HKU**, **HKDD** и некоторые **HKLM** с соответствующими кустами **HKLM\HARDWARE** и **HKLM\SYSTEM\Clone**. ОС создает их каждый раз при загрузке и хранит в оперативной памяти до момента завершения сеанса работы.

Таблица 4.2. Корневые ключи Реестра ОС Windows XP

№ п/п.	Ключ	Описание
1.	**HKCR**	**HKEY_CLASSES_ROOT.** Подключи этого корневого ключа содержат основную информацию о типах файлов, зарегистрированных в системе. Названия подключей совпадают с соответствующими расширениями файлов. Корневому ключу **HKCR** подчиняются описания различных программных средств обработки этих файлов, а также сведения обо всех категориях зарегистрированных объектов.
2.	**HKCU**	**HKEY_CURRENT_USER.** Эта категория содержит описание параметров, меняющихся в зависимости от профиля пользователя, в данный момент работающего в системе. Изменения, относящиеся к текущему пользователю, следует всегда вносить именно сюда, так как они автоматически копируются для длительного хранения при завершений работы компьютера и восстанавливаются в ходе начальной загрузки ОС.
3.	**HKLM**	**HKEY_LOCAL_MACHINE.** Этот раздел отвечает за информацию об аппаратных компонентах компьютера и средствах, обеспечивающих их работу. Здесь также хранится общая информация об установленном программном обеспечении.
4.	**HKU**	**HKEY_USERS.** Этот раздел содержит подключи, соответствующие всем пользователям, зарегистрированным на данном компьютере. Когда один из пользователей начинает работу в системе, ОС автоматически копирует соответствующий ключ **HKU** в раздел **HKCU**. При завершении сеанса пользователя данные копируются обратно.

Продолжение таблицы 4.2

5.	**HKCC**	**HKEY_CURRENT_CONFIG.** В этом разделе дублируется информация (текущий набор конфигурационных параметров аппаратуры) о некоторых устройствах компьютера, в первую очередь о видеоадаптере и принтере.
6.	**HKDD**	**HKEY_DYN_DATA.** Этот раздел содержит текущую информацию о работе компьютера, обычно обновляемую в режиме реального времени. Основные подключи содержат данные об устройствах, работающих в настоящее время, а также сведения о текущем значении статистических параметров. Отобразить эти данные позволяет служебный модуль **«Системный монитор»**.

Возвращаясь к вопросу о параметрах ключей и их значениях, следует сказать, что каждый ключ содержит как минимум одно значение какого-либо параметра. Как у любого файла в ФС, у параметра значения имеется имя, в то время как расширение файла похоже на его тип. Данные значения по аналогии с ФС похожи на конкретное содержимое файла. Из сказанного следует, что каждый ключ или подключ имеет одно или более значений, в свою очередь, каждое из которых характеризуется именем соответствующего параметра, типом и хранимыми в нем данными. Имя параметра значения (или просто имя значения) представляет собой строку, содержащую до 512 символов в кодировке ANSI (или 256 символов в кодировке Unicode), за исключением символов, зарегистрированных для имен ОС Windows XP. Всего для значений предусмотрено пятнадцать различных типов, три из которых: **REG_BINARY**, **REG_DWORD** и **REG_SZ** являются основными и описывают большинство всех значений в Реестре ОС. Двоичные данные значений типа **REG_BINARY**, записанные в шестнадцатеричном виде, представляют собой строку байтов произвольной длины. Их обычно применяют в том случае, когда параметр должен хранить набор данных определенной структуры. Значения типа **REG_DWORD** имеют длину данных в два машинных слова (четыре байта) и записываются в десятичной или шестнадцатеричной форме. Многие значения в Реестре принадлежат этому типу и используются в качестве логических флагов: 0 или 1, да или нет, истина или ложь; иногда значения этого типа встречаются в миллисекундах (1000 равно 1 секунде), описывающих время. Наконец, значение типа **REG_SZ** представляет собой текст постоянной длины в виде строки символов,

например, "Microsoft Windows XP". Каждая строка заканчивается символом **null**. Приложения не преобразуют значения этого типа, а транслируют и отображают их "как есть".

В практической работе предполагается изучение основных возможностей редактирования Реестра ОС Windows XP, изменения значений параметров его ключей, а также создания резервных копий с целью его дальнейшего восстановления.

4.2. Подготовка к выполнению практической работы

Перед началом выполнения практической работы в среде ОС Windows XP необходимо осуществить следующее:

1) загрузить ОС Windows XP и активировать справочное меню **(Пуск | Справка и поддержка)**;

2) ознакомиться с описанием Реестра и возможностями его применения в ОС Windows XP;

3) ознакомиться с описанием и возможностями служебного программного средства **«Редактор Реестра» (Regedit)**, изучив справочный материал по данному приложению, находящийся в системном каталоге **C:\Windows\Help** в одноименном файле с расширением **.chm**;

4) воспользовавшись ключом **/?**, ознакомиться с описанием и возможностями консольной утилиты **Reg.exe** для работы с Реестром ОС, доступной из командной строки.

4.3. Порядок выполнения практической работы

Для выполнения практической работы необходимо запустить виртуальную машину с гостевой ОС Windows XP.

Порядок выполнения:

Существуют тысячи различных коммерческих приложений и системных утилит, позволяющих вносить в Реестр ОС необходимые изменения. Каким из этих инструментов пользоваться зависит от предпочтений и навыков пользователя. Ниже приведен список некоторых из подобных программных продуктов, по мнению автора, заслуживающих большего внимания.

Основным инструментом, наиболее простым в использовании и доступным сразу же после инсталляции ОС Windows XP, является служебный модуль "**Редактор Реестра" (Registry Editor)**. По существу, этой системной утилиты вполне достаточно для выполнения функций редактирования Реестра ОС. Другим дополнительным инструментом, поддерживающим большинство возможностей Реестра, является консольная системная утилита **Reg.exe**, работающая из командной строки ОС. Ее особенность состоит в том, что она может быть востребована при написании пакетных файлов и использована как любая другая системная команда ОС Windows XP. К комплексным утилитам редактирования Реестра и оптимизации ОС с его помощью относятся, в частности, приложение **RegOrganizer** системного программиста Константина Полякова и мощный пакет **jv16 PowerTools** от компании **MaceCraft Software**. Оба этих комплекта программного обеспечения позволяют редактировать и оптимизировать Реестр, осуществлять поиск и замену различных значений системных параметров, вручную или автоматически осуществлять чистку Реестра, в частности, когда необходимо избавиться от следов деинсталляции ненужных приложений и программ, а также производить "тонкую" настройку Реестра. Помимо отмеченных особенностей пакет программ **jv16 PowerTools** дополнительно содержит различные средства диспетчеризации и управления приложениями и файлами. Все описанные программные средства позволяют производить правку Реестра, конфигурирование и оптимизацию ОС, однако наиболее простым в применении является служебный программный модуль **"Редактор Реестра"**. Поэтому дальнейший ход практической работы предполагается осуществлять с применением этого программного продукта.

Задание № 4.3.1. Изучить способы назначения программы по умолчанию для открытия вновь созданных типов файлов с помощью системного модуля "**Редактор Реестра"** ОС Windows XP.

Дальнейшее изучение возможностей Реестра будет направлено на то из них, которое является прерогативой IT-профессионалов и системных программистов, а именно возможность настройки ассоциаций файлов, позволяющая управлять следующими аспектами их обработки в ОС Windows XP:

- какую пиктограмму ОС отображает рядом с именем файла;
- какое запускается приложение при двойном щелчке мышью;
- как "**Проводник"** отображает конкретные типы файлов в системе;

– какие команды появляются в контекстном меню файла;

– другие функции, например, такие как "всплывающие подсказки".

Когда пользователь щелкает правой кнопкой мыши на текстовом файле и выбирает команду "**Открыть"** из контекстного меню, вначале ОС ищет расширение файла в **HKCR**. Значение по умолчанию указывает на то, что класс программ, ассоциированный с расширением **.txt**, называется **txtfile**. Принимая во внимание эти данные, ОС далее ищет в **HKCR\txtfile** подключ **shell**, чтобы определить команды, которые следует добавить к контекстному меню и запускает команду, указанную в значении подключа **command** (**Shell\Open\command**). Команда в подключе **command** обычно имеет вид "**Исполняемое приложение"**, включающее полный путь и имя исполняемого файла, со следующими за ним опциями (например, %1). **Необходимо помнить**, что при написании скриптов %1 является указателем на целевой файл для открытия (заключите %1 в кавычки на случай, если путь и имя целевого файла содержат пробелы).

В качестве примера к изучаемому материалу, создайте в системном Реестре ОС Windows XP свой собственный обработчик произвольного расширения. Для этого выполните следующие действия:

– придумайте самостоятельно произвольное расширение, состоящее из трех символов, обработчик которого предполагается создать,

– в разделе **HKCR** Реестра ОС создайте новый раздел с названием придуманного ранее расширения; при этом обратите внимание на то, как это уже сделано для других расширений в системе,

– значение строкового параметра (по умолчанию), соответствующего созданному разделу, должно содержать ссылку вида ***file**, где *** – символы выбранного расширения, на раздел обработчика данного расширения,

– в разделе **HKCR** Реестра ОС создайте новый раздел обработчика расширения следующего вида ***file\shell\open\command** – для команды открытия и ***file\shell\list\command** – для команды просмотра файла;

– в расширяемом строковом параметре раздела ***file\shell\list** измените данные значения по умолчанию на **"Мой просмотр"**,

– в соответствующих разделах **command** измените значения расширяемых строковых параметров на команды для открытия файла и его просмотра. В частности, для открытия текстового файла необходимо воспользоваться

приложением **WordPad.exe** (требуется указание полного пути к исполняемому файлу), а для его просмотра выбрать **NotePad.exe**,

– проверьте работоспособность обработчика, выполнив следующее:

а. Откройте любую папку, в которой планируете создать новый файл или изменить существующий.

б. В строке меню выберите последовательно пункты **"Сервис" – "Свойства папки"**. Далее откройте вкладку **"Вид"** и в разделе **"Дополнительные параметры"** снимите галочку в пункте **"Скрывать расширения для зарегистрированных типов файлов"**.

в. Выберите какой-либо файл или создайте новый (непустой) с помощью программы **"Блокнот"** с его стандартным расширением. Имя файла должно содержать **имена студентов**, выполняющих работу, и **номер группы** (например, C:\362-2_Ivanov_Petrov.txt).

г. Поменяйте стандартное расширение на то, обработчик которого Вы только что создали.

д. Правой кнопкой манипулятора мышь выберите из контекстного меню команду с именем того файла (**filename.*****), который Вы собираетесь открыть или команду **"Мой просмотр",** чтобы просмотреть файл; при этом должно загрузиться соответствующее приложение обработчика.

Задание № 4.3.2. Изучить способы настройки внешнего вида ОС Windows XP с помощью системного модуля "**Редактор Реестра"**.

Еще одной специальной возможностью Реестра, которая может существенно упростить восприятие ОС, является возможность настройки ее внешнего вида. В Реестре ОС существуют десятки, если не сотни, различных программных переключателей, позволяющих включить или отключить ту или иную визуальную опцию в системе. В частности, воспользовавшись некоторыми настройками Реестра ОС можно настроить главное меню **"Пуск"**.

Настройка главного меню системы возможна стандартными средствами ОС, в частности, посредством GUI. Хотя в ОС имеется такая возможность, опытные пользователи и IT-профессионалы, возможно, захотят создать скрипт для автоматизации настроек этого меню. Системные администраторы вряд ли будут перенастраивать меню "**Пуск"** при каждой установке ОС Windows XP, особенно,

когда парк обслуживаемых машин исчисляется сотнями. Скорее всего, написанный скрипт будет автоматически распространяться по сети.

Все настройки главного меню "**Пуск**" находятся в системном Реестре в одном месте **HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\ Advanced**. Таблицы 4.3 и 4.4 описывают значения, которые можно добавлять в этот ключ. Причем первая таблица содержит значения для классического меню **"Пуск"**, а вторая – для нового меню, соответственно. Большинство из этих значений принадлежит к типу **REG_DWORD** (данные имеют вид 0x01, 0x02 и т.д.), но некоторые из них имеют тип **REG_SZ** (символьные данные вида "**NO**" или "**YES**").

Таблица 4.3. Настройки классического меню **«Пуск»** ОС Windows XP

№ п/п.	Параметр	Описание
1.	StartMenuAdminTools	**«Администрирование»** **NO** – Скрыть; **YES** – Отобразить;
2.	CascadeControlPanel	**«Панель управления»** **NO** – Отобразить как ссылку; **YES** – Отобразить как меню;
3.	CascadeMyDocuments	**«Мои документы»** **NO** – Отобразить как ссылку; **YES** – Отобразить как меню;
4.	CascadeMyPictures	**«Мои рисунки»** **NO** – Отобразить как ссылку; **YES** – Отобразить как меню;
5.	CascadePrinters	**«Принтеры»** **NO** – Отобразить как ссылку; **YES** – Отобразить как меню;
6.	IntelliMenus	**«Персонифицированное меню»** **0x00** – не использовать; **0x01** – использовать;
7.	CascadeNetwork-Connections	**«Сетевые подключения»** **NO** – Отобразить как ссылку; **YES** – Отобразить как меню;
8.	Start_LargeMFUIcons	**«Пиктограммы в меню «Пуск»** **0x00** – Отобразить маленькими; **0x01** – Отобразить большими;
9.	StartMenuChange	**«drag'n'drop»** **0x00** – Отключить; **0x01** – Включить;
10.	StartMenuFavorites	**«Избранное»** **0x00** – Скрыть; **0x01** – Отобразить;
11.	StartMenuLogoff	**«Завершение сеанса»** **0x00** – Скрыть; **0x01** – Отобразить;
12.	StartMenuRun	**Команда «Выполнить»** **0x00** – Скрыть; **0x01** – Отобразить;
13.	StartMenuScrollPrograms	**Прокрутка меню «Программы»** **NO** – Не использовать; **YES** – Использовать;

Таблица 4.4. Настройки нового меню **«Пуск»** ОС Windows XP

№ п/п.	Параметр	Описание
1.	Start_ShowControlPanel	**«Панель управления»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
2.	Start_EnableDragDrop	**«drag'n'drop»** **0x00** – Отключить: **0x01** – Включить;
3.	StartMenuFavorites	**«Избранное»** **0x00** – Скрыть; **0x01** – Отобразить;
4.	Start_ShowMyComputer	**«Мой компьютер»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
5.	Start_ShowMyDocs	**«Мои документы»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
6.	Start_ShowMyMusic	**«Моя музыка»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
7.	Start_ShowMyPics	**«Мои рисунки»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
8.	Start_ShowNetConn	**«Сетевые подключения»** **0x00** – Скрыть; **0x01** – Отобразить как ссылку; **0x02** – Отобразить как меню;
9.	Start_AdminToolsTemp	**«Администрирование»** **0x00** – Скрыть; **0x01** – Отобразить в меню «Все программы» **0x02** – Отобразить в меню «Все программы» и меню «Пуск»;
10.	Start_ShowHelp	**«Справка и поддержка»** **0x00** – Скрыть; **0x01** – Отобразить;
11.	Start_ShowNetPlaces	**«Сетевое окружение»** **0x00** – Скрыть; **0x01** – Отобразить;

Продолжение таблицы 4.4.

№ п/п.	Параметр	Описание
12.	Start_ShowOEMLink	**«Производитель»** **0x00** – Скрыть; **0x01** – Отобразить;
13.	Start_ShowPrinters	**«Принтеры и факсы»** **0x00** – Скрыть; **0x01** – Отобразить;
14.	Start_ShowRun	**Команда «Выполнить»** **0x00** – Скрыть; **0x01** – Отобразить;
15.	Start_ShowSearch	**Команда «Найти»** **0x00** – Скрыть; **0x01** – Отобразить;
16.	Start_ScrollPrograms	**Прокрутка меню «Программы»** **0x00** – не использовать; **0x01** – использовать;

Для выполнения данного задания выберите **не менее 5 параметров из каждой таблицы**. В случае отсутствия в реестре необходимого параметра создайте его самостоятельно с нужным значением.

Рассмотренные в предыдущей и в данной практической работе некоторые частные вопросы являются минимально необходимыми и достаточными для того, чтобы показать широкие возможности системного Реестра ОС Windows XP. Изучение Реестра ОС и инструментов для работы с ним является одной их важнейших задач при обучении IT-профессионалов и опытных пользователей, поскольку в дальнейшем позволит им, не прибегая к стандартным программным средствам ОС, оперировать системными настройками и фактически иметь низкоуровневый доступ к ОС. К сожалению, в рамках практической работы изучение всех возможностей Реестра не представляется возможным. Тем не менее, в глобальной сети Интернет на эту тему существует огромное количество литературы, конкретных системных настроек Реестра, твиков и скриптов на его основе, а также практических рекомендаций по конфигурированию ОС.

5. Мониторинг и оптимизация ОС Windows XP

Цель работы: Изучить основные инструменты консоли администрирования, предназначенные для диагностики, мониторинга, настройки, оптимизации и аудита ОС Windows XP.

5.1. Краткие теоретические сведения

На сегодняшний день в сфере информационных технологий существует множество утилит различных производителей, ориентированных на мониторинг и оптимизацию операционной среды, диагностику и исправление конфликтных ситуаций в системе, получения динамических характеристик работы аппаратно-программных средств компьютера, а также аудит различных категорий событий, в частности, предназначенных для обеспечения системной безопасности. Поскольку ОС изначально не настроена производителем оптимально, операции ее диагностики, настройки и оптимизации представляют интерес для любого пользователя. С этой точки зрения, ценным представляется способность программного обеспечения (ПО) самостоятельно находить оптимальное решение по настройке ОС с возможностью подробного разъяснения результатов оптимизации. Для этого существует целый класс ПО, способный непосредственно диагностировать и анализировать полученные результаты с выдачей некоторых оптимальных рекомендаций по улучшению работоспособности системы. К наиболее популярным наборам такого рода ПО относятся программные комплексы или пакеты типа **Everest** от компании Lavalys и **Norton System Works** от Symantec. Первый пакет программ представляет собой мощное средство анализа и диагностики, а также создания отчетов с целью выявления «узких мест» ОС, однако, он не содержит собственных средств для исправления обнаруженных дефектов системы. Второй – напротив, наряду со средствами диагностики, содержит утилиты для упреждающего обнаружения и исправления ошибок ОС с целью ее дальнейшей оптимальной работы. В совокупности эти два программных средства обеспечивают надежное и безошибочное функционирование операционной среды. Следует отметить, что кроме указанных существует ряд аналогичных программных пакетов, ничем не уступающих им, а иногда даже превосходящих по эффективности выполнения процедур диагностики, мониторинга и оптимизации ОС.

Операционные системы семейства Windows также имеют достаточно широкий набор встроенных штатных средств (системных модулей), предназначенных для диагностики и оптимизации. Эти средства, к числу которых, прежде всего, относятся специализированные оснастки и расширения, могут быть интегрированы в консоль администрирования MMC и использованы системным администратором для контроля процессов, происходящих в операционной среде. Кроме того, существует ряд системных модулей предназначенных преимущественно для получения сведений о системе и настройке ее основных параметров. Некоторые из основных возможностей указанных программных средств будут более подробно рассмотрены в ходе выполнения настоящей практической работы.

5.2. Подготовка к выполнению практической работы

Прежде чем создавать новую консоль администрирования, необходимо определить действия, для которых предназначена эта консоль, список администрируемых компонентов, оснасток и других элементов, которые потребуются для выполнения поставленных перед администратором задач. Необходимо оценить какие именно компоненты будут использованы для мониторинга ОС, ее диагностирования и, возможно, аудита системных процессов и событий. Отдельно, следует рассмотреть необходимость создания видов панели задач. После принятия этих решений можно открыть новую консоль и начать добавлять элементы к ее дереву. Полное руководство по созданию и настройке консолей MMC находится на Web-узле корпорации Майкрософт (**http://www.microsoft.com**). На основе полученных ранее знаний по организации и построению консоли MMC, в настоящей практической работе предполагается осуществить изучение базовых возможностей некоторых инструментов диагностики, мониторинга, настройки, оптимизации и аудита ОС Windows XP.

Перед началом выполнения практической работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню **(Пуск | Справка и поддержка)**;

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с описанием и возможностями системных модулей **Taskmgr, Msinfo32**, **Dxdiag** и **Msconfig,** изучив справочный материал, находящийся в системном каталоге **C:\Windows\Help** в одноименных файлах с расширением **.chm**;

4) ознакомиться с описанием и возможностями оснасток, предназначенных для диагностики, мониторинга, настройки и оптимизации ОС Windows XP: **«Производительность» («Системный монитор»)**, **«Службы»**, **«Диспетчер устройств»**, **«Управление дисками»**, **«Дефрагментация диска»**.

5) ознакомиться с описанием и возможностями оснасток, предназначенных для организации аудита системных процессов и событий в ОС Windows XP: **«Групповая политика»**, **«Просмотр событий»**.

5.3. Порядок выполнения практической работы

Практическая работа выполняется последовательно в соответствии с определенным порядком и включает в себя два учебных задания. Для выполнения практической работы необходимо использовать виртуальную машину.

На основе полученных ранее знаний и навыков по организации и построению консоли администрирования ММС необходимо выполнить следующее:

I. Создайте новую консоль администрирования в авторском режиме.

II. Сконфигурируйте параметры созданной консоли должным образом с целью придания ей уникального вида. Назовите консоль именем, отражающим **фамилию и группу студента**, выполняющего работу.

III. Добавьте на консоль новую панель вида задач, следуя инструкциям **«Мастера создания вида панели задач»**.

В процессе работы **«Мастера»** введите новое имя «Мониторинг и оптимизация» и описание «Системные модули и команды» для данной панели задач.

IV. При завершении работы мастера создания вида панели задач, установив соответствующий флажок, запустите **«Мастер создания новой задачи»**.

V. В процессе работы **«Мастера создания новой задачи»:**

– выберите тип команды **«Команда операционной системы»**, чтобы в дальнейшем обеспечить запуск интегрируемых в консоль администрирования программ и команд,

– в графе **«Команда»** следующего окна введите **Taskmgr**,

– далее в графе **«Название задачи»** введите «Диспетчер задач»,

– при завершении работы мастера создания задачи, запустите его повторно, установив соответствующий флажок на последнем окне.

VI. Повторите работу мастера создания задачи и аналогичным образом дополнительно подключите системные модули, название и описание которых представлено ниже (табл. 5.1). С помощью данного набора системных инструментов администратор сети может оперативно получать основную информацию об аппаратно-программных средствах ОС Windows XP, осуществлять ее диагностику и мониторинг, а в некоторых случаях производить действия по ее настройке и оптимизации.

Таблица 5.1. Основные системные модули диагностики и мониторинга, настройки и оптимизации ОС Windows XP

№ п/п.	Системный Модуль	Описание
1.	**Модуль:** Taskmgr.exe **Название:** Диспетчер задач	Отображает ключевые показатели выполняемых процессов и компьютера в целом. При этом имеется возможность просмотра активности выполняющихся процессов с использованием до 15 параметров, а также графиков и сведений об использовании ЦП и памяти. Имеется возможность принудительного завершения процесса в случае необходимости. При подключении к сети, имеется возможность просматривать состояние и параметры ее работы.
2.	**Модуль:** Msinfo32.exe **Название:** Сведения о системе	Отображает данные о конфигурации системы, включая информацию о конфигурации оборудования, компонентах компьютера, а также программном обеспечении, как для локальных, так и для удаленных компьютеров.
3.	**Модуль:** Dxdiag.exe **Название:** Диагностика DirectX	Отображает сведения о компонентах и драйверах интерфейса прикладного программирования приложений (API) Microsoft DirectX в системе. Позволяет проверить работу звуковой и графической подсистем.
4.	**Модуль:** Msconfig.exe **Название:** Настройка Системы	Позволяет изменять конфигурацию ОС путем отключения (включения) системных компонентов и программных модулей, оптимизировать ее работу, а также автоматизировать устранение неполадок при ее настройке.

Примечание. Системные модули (табл. 5.1) могут быть также открыты с помощью командной строки **Выполнить** в меню **Пуск.** Дополнительная справочная информация об изучаемых инструментах диагностики, мониторинга и конфигурирования ОС доступна в меню **«Справка»** соответствующих системных модулей, а также в справочной системе ОС Windows XP **(Пуск | Справка и поддержка).**

Задание №5.1. Изучить основные возможности получения системной информации диагностики и мониторинга ОС Windows XP, а также элементарные действия по ее конфигурированию и оптимизации на конкретных примерах.

Секция А. Ознакомление с системными модулями, предназначенными для диагностики и мониторинга ОС Windows XP. К числу основных системных модулей диагностики и мониторинга ОС относятся модули **Msinfo32.exe**, **Dxdiag.exe**, а также универсальный модуль **Taskmgr.exe**, позволяющий не только отслеживать основные ресурсы системы, но и вносить некоторые конфигурационные изменения в их работу (например, изменение приоритетов системных и пользовательских процессов, находящихся в оперативной памяти). Для ознакомления с возможностями диагностики и мониторинга ОС посредством указанных системных модулей выполните следующее.

1. Откройте только что созданную консоль администрирования и дважды кликнув мышью на каждом из названий **«Сведения о системе»**, **«Диагностика DirectX»** и **«Диспетчер задач»**, вызовите соответствующие системные модули для выполнения задач диагностирования и мониторинга ОС Windows XP. Сверните их на панель задач.

2. Разверните окно модуля **«Сведения о системе»** и последовательно просмотрите все категории сведений. При этом обратите внимание на то, что глобально все категории делятся на четыре класса «Ресурсы аппаратуры», «Компоненты», «Программная среда» и «Параметры обозревателя». Наиболее полезными с точки зрения сетевого администрирования являются категории «Конфликты/Совместное использование» и «Прерывания» в классе «Ресурсы аппаратуры», категория «Сеть» в классе «Компоненты», а также категории «Переменные среды», «Сетевые подключения» и «Службы» в классе «Программная среда». Необходимо отметить, что указанные классы ресурсов являются ценным источником системной информации, поскольку позволяют отслеживать аппаратные и программные изменения как локально, так и удаленно. Последнее может быть осуществлено посредством выбора **«Удаленный компьютер…»** в меню **«Вид»**. Кроме того, отдельный интерес может представлять информация, собранная в классе «Параметры обозревателя».

3. Выберите **«Журнал сведений о системе»** в меню **«Вид»** и изучите его на предмет какие ресурсы аппаратуры и программные компоненты задействованы в текущий момент в системе.

4. Одним из очень важных программных компонентов рассматриваемого системного модуля диагностики является **«Диагностика сети»**, располагающийся в

меню **«Сервис»**. Компонент **«Диагностика сети»** позволяет выполнить различные тесты и собрать информацию о сети. В зависимости от выбранных параметров, компонент тестирует сетевое взаимодействие и проверяет доступность некоторых сетевых служб и программ, а также производит сбор основной информации о компьютере. Это средство предоставляет системному администратору информацию необходимую для поиска причин, вызвавших проблемы с сетью.

5. Запустите программный компонент **«Диагностика сети»**, кликнув по нему мышью. Настройте **«Параметры сбора информации»**, отметив последовательно все действия и категории флажками, и соберите информацию об оборудовании, программном обеспечении и сетевых подключениях, кликнув по соответствующей гипертекстовой ссылке в текущем окне. Изучите собранную информацию и сохраните гипертекстовый файл для отчета.

6. Разверните окно следующего системного модуля **«Диагностика DirectX»**, предназначенного для диагностирования аппаратных и программных компонентов компьютера, применяющихся для поддержки средств мультимедиа в играх и фильмах, и последовательно изучите все его вкладки. На вкладках **«Дисплей»**, **«Звук»** и **«Музыка»** осуществите проверку соответствующих программных составляющих DirectX, а именно, интерфейсов DirectDraw, DirectSound и DirectMusic. Сохраните все сведения в текстовый файл для отчета. Обратите внимание на то, что системный модуль **«Диагностика DirectX»** также может быть вызван из меню **«Сервис»** программного модуля **«Сведения о системе»**.

7. Универсальный системный модуль **«Диспетчер задач»,** как правило, является наиболее часто используемым компонентом ОС, предназначенным для диагностики и мониторинга основных аппаратно-программных ресурсов системы, таких как центрального процессора, оперативной памяти, системных процессов. В частности, этот модуль позволяет управлять приложениями и процессами в оперативной памяти, снимать их с выполнения и назначать новое значение класса приоритета. Разверните окно системного модуля **«Диспетчер задач»** и последовательно ознакомьтесь со всеми его вкладками и меню.

Выполните следующие действия:

– на вкладках **«Приложения»** и **«Процессы»** обратите внимание на количество работающих приложений и активных процессов,

– рядом с системным модулем **«Диспетчер задач»** разверните модуль **«Сведения о системе»** и откройте категорию «Выполняемые зада-чи» в классе «Программная среда»,

– в меню **«Вид»** в модуле **«Диспетчер задач»** добавьте следующие столбцы счетчиков: «память – максимум», «объем виртуальной па-мяти», «базовый приоритет», «счетчик потоков»,

– в модуле **«Диспетчер задач»** измените базовый приоритет процесса **Dxdiag.exe** на приоритет реального времени, перейдите в окно модуля **«Сведения о системе»**, в меню **«Вид»** обновите системную информацию и обратите внимание на то, как изменилось значение в столбце «Приоритет» в категории «Выполняемые задачи»**,**

– на вкладке **«Приложения»** снимите с выполнения задачи **«Сведения о системе»** и **«Средства диагностики DirectX»,** а на вкладке **«Процессы»** завершите процесс **Taskmgr.exe.**

8. Не закрывая консоль администрирования MMC, сохраните ее. При выполнении заданий секции используйте следующие инструкции:

Секция В. Ознакомление с основным системным модулем, предназначенными для конфигурирования и оптимизации ОС Windows XP.

Одним из основных системных модулей конфигурирования и оптимизации ОС Windows XP является модуль **Msconfig.exe**. Основное его преимущество заключается в том, что он позволяет получить доступ к основным конфигурационным файлам ОС (**System.ini, Boot.ini** и **Win.ini**) без применения дополнительных программных средств. Модуль **Msconfig.exe** является штатным средством диагностики и устранения неполадок загрузки ОС. Эта программа позволяет изменять конфигурацию системы путем отключения некоторых компонентов с помощью флажков, что снижает риск опечаток при наборе текстов системных пакетных файлов типа **Boot.ini**. Кроме того, данный модуль обеспечивает возможность изменения количества загружаемых системных служб и приложений автозагрузки в момент старта ОС, что при определенных условиях может быть использовано для оптимизации и контроля аппаратно-программных ресурсов системы. Для

ознакомления с возможностями настройки и оптимизации ОС посредством указанного системного модуля выполните следующее.

1. Откройте созданную консоль администрирования и дважды кликнув мышью на названии **«Настройка системы»** вызовите соответствующий системный модуль для выполнения задач конфигурирования ОС.

Внимание! Будьте предельно аккуратны с изменениями, производимыми в изучаемом системном модуле. Непродуманные действия могут привести к краху операционной системы.

2. Разверните окно модуля **«Настройка системы»**, если оно находится в свернутом состоянии на панели задач. Последовательно изучите все вкладки системного модуля и, в частности, обратите внимание на то, что на вкладке **«Общие»** имеется несколько возможностей загрузки ОС, а на вкладках конфигурационных файлов имеются возможности по изменению системных параметров, влияющих на ход загрузки системы.

3. Как известно, при своей загрузке ОС Windows XP осуществляет автозапуск большого количества системных служб, которые в дальнейшем будут резидентно находится в оперативной памяти и тем самым занимать ее в течение всего сеанса работы ОС. Безусловно, часть из загружаемых в оперативную память системных служб является критически важными для корректной работы ОС, однако, имеется ряд служб, которые, находясь в памяти, могут оказаться невостребованными в процессе работы. Эти службы могут быть отключены изначально и исключены из процесса загрузки в оперативную память. Полный список системных служб ОС Windows XP можно найти в глобальной сети Интернет, изучив который, в дальнейшем принять решение по поводу отключения части ненужных. Данное обстоятельство позволит ускорить запуск ОС и обеспечить некоторую экономию аппаратных ресурсов. На вкладке **«Службы»** отключите две штатные службы ОС Windows XP **«Темы»** и **«Автоматическое обновление»**, убрав соответствующие флажки напротив каждой из них. Нажмите **Применить**, выйдите из системы и снова войдите в нее.

Верните ОС в исходное состояние, выбрав вариант **«Обычный запуск»** на вкладке **«Общие»** или вручную включите ранее отключенные системные службы. Следует отметить, что все службы ОС Windows XP могут быть доступны для конфигурирования и оптимизации из одноименной оснастки **«Службы»**, которая будет рассмотрена позднее в рамках настоящей практической работы.

5. Еще одним элементом, позволяющим сократить время загрузки ОС и оптимизировать ее работу, является группа программ **«Автозагрузка»**. На одноименной вкладке отображаются резидентные программные модули автоматического запуска, помещаемые при загрузке ОС в оперативную память. Убрав соответствующие флажки напротив лишних программных модулей можно исключить их из процесса загрузки ОС. Такими ненужными модулями могут оказаться части инсталлируемых приложений, отвечающие за их автоматический запуск, например, при обращении к аппаратуре компьютера. Частным примером может служить программный элемент автозагрузки, отвечающий за автоматический запуск программного проигрывателя при обращении к приводу DVD. Его наличие в группе **«Автозагрузка»** и, следовательно, в оперативной памяти, не всегда оправданно, поскольку программа, проигрывающая диски DVD, может быть запущена вручную из меню Пуск по желанию пользователя.

Внимание! При отключении ненужного программного элемента автозагрузки необходимо четко представлять, за что этот элемент отвечает. Отключение необходимого системе компонента может привести к невозможности ее загрузки. На вкладке **«Автозагрузка»** отключите выбранный элемент автозагрузки, убрав соответствующий флажок. Нажмите **Применить**, выйдите из системы и снова войдите в нее. Верните ОС в исходное состояние, выбрав вариант **«Обычный запуск»** на вкладке **«Общие»** или вручную включите ранее отключенный элемент автозагрузки.

6. Не закрывая консоль администрирования MMC, сохраните ее.

VII. Кроме рассмотренных в предыдущих заданиях системных модулей в ОС Windows XP имеются дополнительные штатные средства, позволяющие производить мониторинг и оптимизацию системы не прибегая к внешним утилитам. К их числу, как уже утверждалось ранее, относятся оснастки **«Производительность»** (**«Системный монитор»**), **«Службы»**, **«Диспетчер устройств»**, **«Управление дисками»**, **«Дефрагментация диска»**, а также их расширения, которые могут быть добавлены на созданную консоль администрирования. Наряду с изученными системными модулями эти средства представляют собой пакет программного обеспечения, ориентированного на выполнение задач диагностики, мониторинга, настройки и оптимизации ОС. Основные особенности рассматриваемых программных средств представлены ниже.

Оснастка **«Системный монитор»** служит для сбора в реальном времени и просмотра данных памяти, диска, процессора, сети и других параметров в виде графика, гистограммы или отчета. В совокупности с компонентом **«Оповещения и журналы производительности»**, с помощью которого настраиваются журналы для записи данных и устанавливаются системные оповещения о значениях счетчиков, оснастка **«Системный монитор»** представляет собой программное средство, называемое **«Производительность»**, являющееся штатной утилитой ОС Windows XP и предназначенное для диагностики и мониторинга системы. Более подробно работа с оснасткой "Системный монитор" будет рассмотрена на одной из следующих практических работ.

Оснастка **«Диспетчер устройств»** предоставляет сведения об установленном на компьютере оборудовании и его настройках, а также о взаимодействии этого оборудования с программными средствами системы. С помощью нее можно обновлять драйверы установленного на компьютере оборудования, изменять их настройки, а также устранять некоторые программные неполадки.

Служебная программа **«Управление дисками»** и одноименная оснастка предназначены для управления жесткими дисками и содержащимися на них разделами и томами. С помощью этой программы можно инициализировать новые диски, создавать тома, а также форматировать их с целью дальнейшего использования файловых систем FAT, FAT32 или NTFS. Программа **«Управление дисками»** позволяет выполнять задачи по работе с дисками без перезагрузки компьютера, так как большинство изменений вступает в силу незамедлительно.

Как и предыдущая служебная программа, системный модуль **«Дефрагментация дисков»** представляет собой автономную утилиту, но также может быть добавлен на консоль администрирования в виде оснастки. Работа этой утилиты заключается в объединении фрагментированных файлов и папок на жестком диске, после чего каждый файл или папка тома занимает единое непрерывное пространство. Этот процесс называется дефрагментацией, который, с точки зрения оптимизации работы ОС и эффективного доступа к данным на жестком диске, является критически важным. Кроме того, дефрагментация, объединяя в единое целое свободное место на жестком диске, делает менее вероятной фрагментацию новых файлов в системе.

Еще одним средством, направленным на оптимизацию работы ОС и уже частично рассмотренным выше, является оснастка **«Службы»**, помогающая

управлять службами компьютера, настраивать действия по восстановлению службы в случае ее сбоя, а также создавать пользовательские имена и описания для служб с целью простоты ориентации в системе. Дополнительная информация по данной тематике доступна в разделах **«Использование консоли «Производительность»**, **«Использование «Системного монитора»**, **«Использование оснастки «Службы»**, **«Использование диспетчера устройств»**, **«Использование оснастки «Управление дисками»**, а также **«Использование программы дефрагментации дисков»** справки ОС Windows XP (**Пуск | Справка и поддержка**).

Задание №5.2. Изучить основные возможности оснасток, предназначенных для диагностики, мониторинга, настройки и оптимизации ОС Windows XP на конкретных примерах.

Секция А. Ознакомление с основными возможностями оснастки **«Диспетчер устройств»** в ОС Windows XP.

Программный модуль **«Диспетчер устройств»** главным образом представляет собой средство, предназначенное для диагностики и мониторинга аппаратных составляющих компьютера и их взаимосвязь с соответствующими программными компонентами (драйверами) в системе. Использование **«Диспетчера устройств»** позволяет легко определить, какое оборудование установлено в системе и какие устройства нуждаются в установке подходящего драйвера для корректной работы. Для ознакомления с возможностями диагностики аппаратных средств ОС Windows XP с использованием оснастки **«Диспетчер устройств»** выполните следующее.

1. Локально добавьте на открытую консоль администрирования новую системную оснастку **«Диспетчер устройств»**.

2. Воспользовавшись установленной оснасткой **«Диспетчер устройств»,** ознакомьтесь с деревом отображенных по типу системных устройств и обратите внимание на устройства, помеченные уведомляющим треугольным знаком желтого цвета, если таковые присутствуют в системе.

3. Изучите меню **«Вид»** оснастки **«Диспетчер устройств»** и обратите внимание на то, что системные устройства отличаются от ресурсов системы.

4. Выберите любые четыре устройства системы, определите, какой драйвер управляет каждым из них, имеет ли он цифровую подпись и какие аппаратные ресурсы при этом использует.

5. Не закрывая консоль администрирования MMC, сохраните ее.

Секция В. Ознакомление с основными возможностями оснасток «Управление дисками» и «Дефрагментация дисков» в ОС Windows XP.

Обе оснастки **«Управление дисками»** и **«Дефрагментация дисков»** в совокупности представляют собой средство диагностики и оптимизации одной из основных подсистем ОС, а именно, подсистемы ввода/вывода. Подсистема ввода/вывода и файловая система как ее составляющая часть являются одним из основных средств обмена информацией в ОС. Поэтому диагностика и оптимизация данной подсистемы представляет критически важный и периодически необходимый процесс. С этой целью наиболее эффективным является регулярное применение дефрагментации жесткого диска, способствующее упорядочиванию информации на носителе, что, в свою очередь, позволяет иметь минимальное время доступа к данным. Для ознакомления с возможностями диагностики и оптимизации подсистемы ввода/вывода в ОС Windows XP посредством применения оснасток **«Управление дисками»** и **«Дефрагментация дисков»** выполните следующее.

1. Локально добавьте на открытую консоль администрирования новые системные оснастки **«Управление дисками»** и **«Дефрагментация дисков»**.

2. Воспользовавшись меню **«Вид»** оснастки **«Управление дисками»**, ознакомьтесь со структурой установленного в подсистеме ввода/вывода оборудования и ее графическим представлением. Обратите внимание на различные способы представления информации о дисковых накопителях, установленных в системе.

3. Одним из актуальных при установке ОС системных инструментов изучаемой оснастки является программное средство, позволяющее изменять букву логического диска в системе. Это средство применяется в случае, когда пользователь решает изменить порядок отображения томов и закрепленных за ними букв, назначенных ОС в процессе ее инсталляции. Измените букву «D:» соответствующего логического диска на «T:», воспользовавшись подпунктом **«Все задачи | Изменить букву диска…»** меню **«Действие»** оснастки **«Управление**

дисками». При необходимости измените обратно системную букву логического диска на **«D:».**

4. Откройте **«Свойства»** в меню **«Действие | Все задачи»** любого, выбранного Вами, логического диска в дополнительном разделе физического диска. Выполните следующие действия:

– на вкладке **«Общие»** присвойте новую метку выбранного тома;

– обратите внимание на возможность сжатия диска для экономии места, которое активируется установкой соответствующего флажка на вкладке **«Общие»**;

– на вкладке **«Общие»** произведите очистку диска, воспользовавшись соответствующей одноименной процедурой;

– на вкладке **«Доступ»** откройте общий доступ к выбранному диску;

– на вкладке **«Оборудование»** обратите внимание на установленные в системе физические накопители и их тип;

– на вкладке **«Сервис»** проверьте выбранный том на наличие системных ошибок с учетом автоматического их исправления, проверкой и восстановлением поврежденных секторов.

5. Обратите внимание на то, что на вкладке **«Сервис»** имеется системная опция, позволяющая осуществить дефрагментацию выбранных логических дисков. С другой стороны, доступ к возможностям программного модуля **«Дефрагментация дисков»** также возможен посредством подключенной ранее одноименной оснастки. Учитывая данное обстоятельство, системный администратор может разделять функции консоли диагностики, мониторинга и оптимизации на этапе ее создания. Разверните окно оснастки **«Дефрагментация дисков»** и проанализируйте все существующие системные тома на предмет выявления наиболее фрагментированного из них. Осуществите дефрагментацию того тома, который имеет максимальный процент фрагментированных данных.

6. Не закрывая консоль администрирования MMC, сохраните ее.

Секция С. Ознакомление с основными возможностями оснастки «Службы» в ОС Windows XP.

Оснастка **«Службы»** является штатным программным средством ОС, предназначенным для администрирования системных служб и служебных приложений, загружаемых резидентно в оперативную память компьютера. Администрирование служб осуществляется посредством подконтрольного ручного

или автоматического включения, а также отключения в случае отсутствия необходимости их наличия в системе. При стандартной установке ОС многие службы настраиваются как **«автоматические»** (запуск служб выполняется автоматически при запуске ОС или при первом обращении к службе). Если для службы задан параметр **«вручную»**, службу необходимо запускать вручную перед осуществлением ее загрузки операционной системой и предоставлением возможности ее использования. Если служба **«отключена»**, ее нельзя запустить ни вручную, ни автоматически. Следует помнить, что изменение стандартной настройки служб может привести к неправильной работе ключевых служб. Особенно важно соблюдать осторожность при изменении параметров **«Тип запуска»** и **«Вход в систему»** для служб, настроенных для автоматического запуска. Если в результате изменения настроек службы возникли неполадки при перезагрузке компьютера, необходимо попытаться перезагрузить его повторно, но в безопасном режиме и изменить настройки службы на начальные или восстановить настройки по умолчанию. Уместно отметить, что у каждой службы имеются определенные разрешения, которые могут быть предоставлены или запрещены для каждого пользователя или группы (табл. 5.2). Разрешения отдельных служб могут быть установлены посредством использования средства **«Шаблоны безопасности»**.

Таблица 5.2. Разрешения служб в ОС Windows XP

№ п/п.	Разрешение	Описание
1.	Полный доступ	Автоматически предоставляет пользователю все служебные разрешения
2.	Запрос шаблона	Определяет настройку параметров, соответствующих объекту службы
3.	Изменение шаблона	Изменяет настройки службы
4.	Запрос состояния	Предоставляет сведения о состоянии службы
5.	Перечисление зависящих служб	Определяет все службы, зависящие от выбранной службы.
6.	Пуск	Запускает службу
7.	Остановка	Останавливает работу службы
8.	Приостановка и продолжение работы	Приостанавливает и продолжает работу службы
9.	Опрос службы	Докладывает текущее ее состояние
10.	Пользовательский элемент управления	Посылает запрос пользовательского элемента управления службе.
11.	Удаление	Удаляет службу
12.	Чтение разрешений	Читает разрешения безопасности, назначенные службе
13.	Смена разрешений	Меняет разрешения безопасности, назначенные службе
14.	Смена владельца	Изменяет ключ безопасности или разрешение для службы, не принадлежащей пользователю

Службы должны входить в ОС с определенной учетной записью, чтобы получить доступ к ее ресурсам и объектам. Некоторые службы по умолчанию настроены на **«Вход в систему»** с локальной системной учетной записью (**«Локальная система»**), которая является самой мощной и имеет полный доступ к системе. Другие службы настроены на **«Вход в систему»** с учетными записями **«Локальная служба»** и **«Сетевая служба»**, которые являются штатными и сходными с проверенными учетными записями пользователей. У этих записей уровень доступа к ресурсам и объектам ОС такой же, как и у членов групп **«Пользователи»** (такое ограничение доступа позволяет защитить систему, если нарушена работа отдельных служб или процессов). Их отличие состоит в том, что

службы с учетной записью **«Локальная служба»** имеют доступ к сетевым ресурсам без применения учетных данных компьютера и, напротив, запись **«Сетевая служба»** обеспечивает доступ к сетевым ресурсам с применением таковых. Полный список стандартных служб при обычной установке ОС Windows XP вместе с настройкой запуска этих служб по умолчанию представлен в разделе **«Стандартные настройки служб»** меню **«Справка»** изучаемой оснастки.

В продолжение ранее поставленного вопроса о настройке ОС Windows XP ознакомьтесь с возможностями ее оптимизации посредством ис-пользования оснастки **«Службы»,** выполнив следующее.

1. Локально добавьте на открытую консоль администрирования новую системную оснастку **«Службы»**.

2. Откройте изучаемую оснастку и ознакомьтесь с полным списком служб, присутствующих в ОС, их описанием, состоянием, типом запуска и «входом от имени». Обратите внимание на то, что состояние службы **«Работает»** соответствует только ее автоматическому запуску.

3. Выберите службу **«Темы»** и настройте ее, выполнив следующие действия:

– щелкните правой кнопкой манипулятора мышь на службе и выбери-те команду **«Свойства»**,

– на вкладке **«Общие»** выберите необходимый «Тип запуска»,

– на вкладке **«Вход в систему»** выберите один из четырех вариантов входа: **1)** «С системной учетной записью», если предполагается использование учетной записи «Локальная система», **2)** в поле «С учетной записью» необходимо ввести **NT AUTHORITY\Local-Service**, если предполагается использовать учетную запись «Локальная служба» или **3)** ввести **NT AUTHORITY\NetworkService**, если предполагается использование записи «Сетевая служба», а также **4)** нажмите кнопку **«Обзор»** и выберите альтернативную учетную запись,

– введите пароль и его подтверждение, в случае необходимости, и нажмите **ОК** для подтверждения ввода.

После перезагрузки компьютера изменения вступят в силу и служба будет работать в настроенном виде.

4. Выберите службу **«Автоматическое обновление»** и осуществите ее остановку, пуск и перезапуск, воспользовавшись меню **«Действие»**. Обратите внимание на то, что при остановке службы, ее состояние изменяется.

5. На примере выбранной самостоятельно службы осуществите настройку действий по ее восстановлению после сбоя (вкладка **«Восстановление»** окна **«Свойства»**). В случае необходимости воспользуйтесь справочным разделом изучаемой оснастки.

6. Самостоятельно выберите три службы из списка и установите зависимости между каждой из них и другими службами ОС (вкладка **«Зависимости»** окна **«Свойства»**). В случае необходимости воспользуйтесь справочным разделом изучаемой оснастки.

7. Как утверждалось ранее, использование оснастки **«Службы»** в качестве инструмента настройки ОС является основополагающим при ее оптимизации. Примером, в частности, может служить увеличение скорости завершения работы ОС Windows XP посредством отключения некоторых неиспользуемых служебных приложений, объединенных общим названием **«Службы терминалов»**. Такими службами являются **«Удаленный рабочий стол»**, **«Удаленный помощник»**, **«Быстрое переключение пользователей»** и **«Терминальный сервер»**. Чтобы вручную настроить эти службы или отключить их как неиспользуемые, выполните следующие действия: найдите **«Службы терминалов»** в списке служб изучаемой оснастки, откройте окно свойств службы, нажмите **«Стоп»**, чтобы остановить работу службы, после чего в поле **«Тип запуска»** выберите **«Отключить»**. Перезагрузите компьютер, чтобы изменения вступили в силу. Аналогичным образом отключаются любые неиспользуемые или невостребованные системой службы или служебные приложения. Это приводит к экономии оперативной памяти, времени работы центрального процессора и, как следствие, к эффективной и оптимальной работе ОС в целом.

8. Сохраните и закройте консоль администрирования MMC.

В настоящей практической работе изучены базовые программные средства, позволяющие осуществлять наблюдение за аппаратно-программными компонентами ОС Windows XP, ее процессами и службами. Рассмотрен комплекс программ, позволяющий настраивать и конфигурировать ОС, осуществлять ее мониторинг и оптимизацию, а также регистрацию системных процессов и событий с

целью обеспечения ее безопасности. Проблема обеспечения безопасности в ОС не ограничивается аудитом системных процессов и событий. Среди прочего, она включает ряд мероприятий по управлению учетными записями (с учетом их блокировки при необходимости), пользователями и группами. Особое внимание следует уделить вопросам безопасности, связанным с целостностью файловой системы и реестра ОС. В заключение следует отметить, что наряду с другими компонентами ОС изученные в практической работе оснастки и служебные модули в совокупности представляют собой единое программное средство системного администратора, называемое **«Управление компьютером»** (**Пуск | Все программы | Администрирование | Управление компьютером**). Использование данного средства и приобретенных в практической работе знаний позволит IT-профессионалам и опытным пользователям получить всю необходимую информацию о системе с целью оценки ее работоспособности и оптимальной настройки ее параметров.

6. Работа с подсистемой безопасности в ОС Windows XP

Цель работы: Изучение основных возможностей подсистемы безопасности и способы защиты данных в среде ОС Windows XP и создание пользовательской консоли администрирования MMC, предназначенной для организации и управления локальными политиками безопасности в среде ОС Windows XP

6.1. Подготовка к выполнению практической работы

Возможность управления политикой безопасности (на локальном компьютере или в сети) осуществляется посредством создания консоли администрирования MMC и добавления на нее соответствующих, предназначенных для этих целей средств управления (оснасток и расширений). При этом возможно использование оснасток, изученных ранее и ориентированных на управление правами доступа и разрешениями, имеющимися у пользователя в процессе работы с локальными ресурсам системы. В случае необходимости, применение других системных инструментов и программных модулей сторонних разработчиков (например, ориентированных на аудит и мониторинг ОС) также может быть полезным с целью расширения функционала консоли администрирования. Средства управления политикой безопасности локального узла, подразделения или домена представлены в табл. 6.1.

Отдельно следует отметить еще одно программное средство **Secedit.exe**, представляющее собой исполняемый файл, запускаемый из командной строки, в рамках пакетного файла или посредством автоматического планировщика заданий. Данное средство используется для автоматизации задач настройки системы безопасности группы компьютеров локальной сети. Для применения данного средства в повседневной практике необходимо иметь навыки использования командного интерпретатора и опыт написания пакетных файлов и сценариев.

Таблица 6.1. Средства управления политикой безопасности ОС

№ п/п.	Средство управления политикой безопасности	Описание
1.	Средство «Локальная политика безопасности»	Данное средство используется для прямого изменения политик учетных записей и локальных политик, политик открытого ключа, а также политик безопасности IP локального компьютера.
2.	Шаблоны безопасности	Шаблон безопасности является файлом, представляющим конфигурацию безопасности или политику безопасности. Подобные шаблоны могут применяться к политике локального компьютера или импортироваться в объект **«Групповая политика»**
3.	Средство «Анализ и настройка безопасности»	Данное средство используется для анализа и настройки безопасности локального узла с помощью шаблона безопасности.
4.	Расширение «Параметры безопасности» для групповой политики	Данное средство может использоваться для изменения отдельных параметров безопасности локального узла, подразделения или домена.

В настоящей практической работе предполагается ознакомление с основными принципами организации локальной и сетевой политик безопасности на основе консоли администрирования MMC с применением базовых возможностей указанных выше программных средств и оснасток «Редактор объекта групповой политики» («Групповая политика»), «Шаблоны безопасности», «Анализ и настройка безопасности», а также «Политики безопасности IP на «Локальный компьютер» и «Монитор IP-безопасности». При этом для детального изучения принципов создания и настройки консоли администрирования MMC с применением отмеченных средств целесообразно воспользоваться полным руководством, находящимся на Web-узле корпорации Майкрософт (http://www.microsoft.com).

Перед началом выполнения практической работы в среде ОС Windows XP необходимо выполнить следующее:

1) загрузить ОС Windows XP и активировать справочное меню (**Пуск | Справка и поддержка**);

2) ознакомиться с описанием и возможностями запуска и применения консоли администрирования MMC;

3) ознакомиться с описанием и возможностями оснасток, предназначенных для организации и администрирования локальной и сетевой политиками безопасности в среде ОС Windows XP: **«Редактор объекта групповой политики» («Групповая политика»), «Шаблоны безопасности», «Анализ и настройка безопасности»,** а также **«Политики безопасности IP на «Локальный компьютер»** и **«Монитор IP-безопасности»**.

6.2. Порядок выполнения практической работы

Практическая работа выполняется последовательно в соответствии с определенным порядком и включает в себя четыре учебных задания.

Практическая работа выполняется в виртуальной машине.

Порядок выполнения

Как было ранее отмечено, локальные политики безопасности применяются на отдельных узлах сети. В состав этих политик входят следующие:

– *Назначение прав пользователя* определяет, какие пользователи и группы обладают правами на вход в систему и авторизованы на выполнение соответствующих задач.

– *Политики аудита* определяют события безопасности, которые, в свою очередь, заносятся в Журнал безопасности данного компьютера. При этом в журнал могут заноситься успешные, неудачные или те и другие попытки. Журнал безопасности является частью оснастки «Просмотр событий».

– *Параметры безопасности* определяют действия ОС, направленные на обеспечение безопасности вычислительной системы. Например, к их числу относятся включение или отключение таких параметров безопасности как цифровая подпись данных, доступ оптическим накопителям, установка определенных драйверов или приглашение на вход в систему. Конфигурирование локальной политики посредством изменения некоторых параметров безопасности будет рассмотрено в ходе выполнения текущей практической работы. При этом необходимо иметь ввиду, что приоритет имеют политики следующих объектов в указанном порядке: подразделение, домен и только затем локальный компьютер.

Это обусловлено тем, что бесконтрольное применение нескольких политик к одному локальному узлу может породить конфликт между параметрами безопасности.

На основе полученных в предыдущих практических работах знаний и навыков по организации и построению консоли администрирования MMC необходимо выполнить следующее:

1. Создайте новую консоль администрирования в авторском режиме, задав ей в качестве имени **фамилию и номер группы студента, выполняющего работу**.

2. При необходимости сконфигурируйте параметры созданной консоли должным образом с целью придания ей уникального вида.

3. Добавьте на консоль новую панель вида задач, следуя инструкциям **«Мастера создания вида панели задач»**. В процессе работы **«Мастера»** введите новое имя **«Политика безопасности»** и описание **«Оснастки и расширения»** для данной панели задач; в появившемся окне **«Завершение мастера создания вида панели задач»** уберите флажок **«Добавить новые задачи на эту панель задач после закрытия мастера»** и нажмите кнопку **«Готово»** для подтверждения операции.

4. Добавьте в корень дерева консоли MMC оснастку **«Локальные пользователи и группы»** и одним из ранее изученных способов создайте новую учетную запись с правами группы **«Пользователи»**. Имя пользователя, описание и пароль выберите самостоятельно. В процессе создания учетной записи пользователя оставьте флажок **«Потребовать смену пароля при следующем входе в систему»**.

5. Не закрывая консоль, сохраните ее.

Последовательность выполненных действий позволяет создать консоль администрирования MMC, придать ей уникальный вид и удобный интерфейс для дальнейшего использования в рамках настоящей практической работы.

Задание №6.1. Изучение основных возможностей программного средства **«Локальная политика безопасности»** в среде ОС Windows XP на конкретных примерах.

Прежде, чем интегрировать инструмент **«Локальная политика безопасности»** на созданную заранее консоль администрирования MMC и осуществить его детальное рассмотрение, необходимо отметить, что в ОС Windows XP данный инструмент существует автономно в виде штатного программного средства и может быть использован на локальном компьютере вне рамок оснастки **«Редактор объекта групповой политики»**. В частности, для просмотра локальной политики безопасности им можно воспользоваться, вызвав его посредством команды **Выполнить** в меню **Пуск**, набрав **secpol.msc** и нажав **Enter** для подтверждения. Кроме того, поскольку модуль **«Локальная политика безопасности»** является штатным средством администрирования, он находится в группе соответствующих программных средств, расположенных в меню **«Пуск | Панель управления | Администрирование»**.

Несмотря на сказанное выше, дальнейшее изучение локальной политики безопасности будет осуществляться в предположении, что имеется системная необходимость создания собственной консоли MMC с включенным внутрь набором необходимых для администрирования инструментов, в том числе модуля **«Локальная политика безопасности»**. Для ознакомления с возможностями локальной политики безопасности в ОС Windows XP с использованием одноименной оснастки, прежде всего, необходимо выполнить следующие подготовительные действия:

1. Откройте только что созданную консоль администрирования MMC, в которой к этому моменту должна быть уже добавлена оснастка **«Локальные пользователи и группы»**.

2. Воспользовавшись оснасткой **«Редактор объекта групповой политики»**, добавьте политику **«Локальный компьютер»** в корень консоли, как было показано в предыдущих практических работах.

3. С одной стороны, в окне дерева консоли MMC откройте ветвь **«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности»** в **«Политике «Локальный компьютер»»**. С другой стороны, в

отдельном окне ОС откройте инструмент **«Локальная политика безопасности»** одним из выше описанных способов и, сравнив содержимое открытых окон, обратите внимание на то, что **«Параметры безопасности»** локальной политики абсолютно идентичны тем, которые отображаются в оснастке **«Политика «Локальный компьютер»**.

Таким образом, у системного администратора появляется возможность в случае необходимости интегрировать базовый инструмент локальной безопасности во вновь создаваемую и конфигурируемую консоль ММС.

4. Сохраните и закройте консоль администрирования ММС.

С целью обучения и ознакомления с **«Локальной политикой безопасности»** интерес в дальнейшем будут представлять **«Политики учетных записей»**, а также некоторые **«Локальные политики»** при **«Назначении прав пользователя»** и общих **«Параметров безопасности»**.

Секция А. Ознакомление с основными возможностями **«Политики учетных записей»** в ОС Windows XP.

Политики учетных записей (**«Конфигурация компьютера | Конфигу-рация Windows | Параметры безопасности | Политики учетных записей»**) применяются на локальных компьютерах сети и определяют взаимодействие учетных записей с данным компьютером или доменом. Существует три политики учетных записей:

– *Политика паролей* определяет параметры паролей, в частности, соответствие набору обязательных условий и сроку их действия.

– *Политика блокировки учетной записи* определяет условия и период времени блокировки учетной записи.

– *Политика Kerberos* определяет параметры протокола сетевой аутентификации Kerberos, такие как срок жизни сеансового билета и соответствие обязательным условиям. Данный протокол обеспечивает взаимно-секретную аутентификацию компьютеров в сети на основе клиент-серверной модели. Политика Kerberos не входит в состав политики локального компьютера, она используется только для учетных записей пользователей домена.

Дополнительная информация по данной тематике доступна в справочных разделах **«Локальная политика безопасности»** и **«Параметры безопасности»** оснастки **«Групповая политика»**, а также в разделе **«Методы проверки**

подлинности» справки ОС Windows XP (**Пуск | Справка и поддержка**) или на сайте **www.oszone.net**.

Для ознакомления с базовыми возможностями **«Политики учетных записей»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Локальные пользователи и группы»** наведите манипулятором мышь на нового пользователя и задайте ему любой пароль, выбрав команду **«Задать пароль...»** из контекстного меню.

2. Найдите подраздел **«Политика паролей»** в разделе **«Политики учетных записей»** оснастки **«Политика «Локальный компьютер»**.

3. Последовательно просмотрите все политики паролей с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

4. Включите политику **«Пароль должен отвечать требованиям сложности»**, изменив положение соответствующего переключателя на вкладке **«Параметр локальной безопасности»**.

5. Установите минимальную длину пароля в 10 символов, осуществив необходимые действия в соответствующей политике паролей.

6. Перейдите в подраздел **«Политика блокировки учетной записи»** и аналогично изучите сущность расположенных здесь политик безопасности.

7. Установите **«Пороговое значение блокировки»** на три ошибки входа в систему и осуществите блокировку учетной записи на 2 минуты в случае совершенных ошибок ввода.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– войдите в систему под созданной учетной записью и проверьте влияние новых значений системных параметров политик безопасности на процесс аутентификации,

– сделайте вывод о проделанной работе и запишите его в отчет.

Секция В. Ознакомление с основными возможностями **«Локальных политик»** при **«Назначении прав пользователя»** в ОС Windows XP.

Локальные политики безопасности, применяемые при назначении прав пользователя (**«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Назначение прав пользователя»**), позволяют системному администратору определить, какие пользователи и группы будут обладать правами на вход в ОС и какие будут при этом авторизованы на выполнение соответствующих задач. Особенностью данных локальных политик является то, что они могут быть применены к любому пользователю или группе в системе простым их (пользователей) добавлением в число тех, на которые рассматриваемая политика распространяется. Это позволяет, тем самым, иметь пользователям возможность влиять на политику безопасности ОС. Для иллюстрации сказанного и ознакомления с базовыми возможностями локальных политик безопасности при **«Назначении прав пользователя»** в ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова. В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Назначение прав пользователя»** в разделе **«Локальные политики»**.

2. Последовательно просмотрите все политики для назначения прав пользователям с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

3. Добавьте созданного ранее пользователя в число тех, которым позволено производить операции архивирования файлов и каталогов в системе. Для этого воспользовавшись одноименной политикой безопасности, **«Добавьте пользователя или группу»** стандартным способом на вкладке **«Параметр локальной безопасности»** и удалите группы, обладающие этим правом по умолчанию.

4. Запретите группам **«Пользователи»** и **«Операторы архива»** доступ к компьютеру из сети. Для этого внимательно изучите политики **«Доступ к компьютеру из сети»** и **«Отказ в доступе к компьютеру из сети»**.

5. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Изменение системного времени»**.

6. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Создание страничного файла»**.

7. Добавьте созданного ранее пользователя в число тех, которым позволено осуществлять **«Управление аудитом и журналом безопасности»**.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– войдите в систему под созданной учетной записью и проверьте влияние новых значений системных параметров политик безопасности на процесс авторизации,

– сделайте вывод о проделанной работе и запишите его в отчет.

Секция С. Ознакомление с основными возможностями **«Локальных политик»** при настройке **«Параметров безопасности»** в ОС Windows XP.

Основные политики, применяемые для обеспечения локальной или сетевой безопасности и представленные в виде набора соответствующих параметров (**«Конфигурация компьютера | Конфигурация Windows | Параметры безопасности | Локальные политики | Параметры безопасности»**), позволяют системному администратору, наряду с политиками учетных записей и базовыми методами авторизации, организовать первый уровень защиты данных от несанкционированного доступа из сети или же, напротив, позволить уполномоченным пользователям иметь определенные права при обращении к информации.

Для ознакомления с базовыми возможностями рассматриваемого набора политик безопасности в ОС Windows XP выполните следующее.

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

В оснастке **«Политика «Локальный компьютер»** найдите подраздел **«Параметры безопасности»** в разделе **«Локальные политики»**.

2. Последовательно просмотрите все политики безопасности данного подраздела с целью их дальнейшего применения на практике. Для этого дважды щелкните на каждой из них и на вкладке **«Объяснение параметра»** изучите их сущность.

3. Включите возможность очистки страничного файла виртуальной памяти при завершении работы системы, воспользовавшись соответствующей политикой безопасности. Это позволит при определенных условиях избежать перехвата данных из виртуальной памяти.

4. Следующие несколько настроек данного пункта задания реализуют концепцию «безопасного входа в систему», которая может быть практически использована на серверах домена или отдельных узлах локальной сети.

Прежде всего, следует отметить, что некоторым пользователям новый механизм входа в систему с использованием окна приветствия в ОС Windows XP может показаться неудобным или непривычным. Для устранения данного дискомфорта в системе имеется вариант переключения данного механизма в «классический» режим. Для этого необходимо осуществить **«Изменение входа пользователей в систему»** в меню **«Пуск | Панель управления | Учетные записи пользователей»**. В появившемся окне необходимо убрать флажки **«Использовать страницу приветствия»** и **«Использовать быстрое переключение пользователей»** и подтвердить изменения, щелкнув манипулятором мышь по кнопке **«Применение параметров»**.

Данное изменение приводит к тому, что после перезагрузки ОС появляется «классическое» окно входа в систему с двумя полями: «Пользователь», в котором следует набрать имя учетной записи, и «Пароль» – для ввода пароля, назначенного этой учетной записи.

Внимание! При переключении механизма входа в «классический» режим утрачивается возможность использования технологии быстрого переключения пользователей. Поэтому, в случае обратного перехода (в положение с использованием окна приветствия) для возврата данной технологии в активное состояние необходимо войти в ОС с правами администратора и установить соответствующий флажок **«Использовать быстрое переключение пользователей»**.

Далее переведите в положение **«Отключено»** параметр безопасности локальной политики **«Интерактивный вход в систему: не требовать нажатия CTRL+ALT+DEL»**, как это делается на рабочих станциях и серверах домена. Эта настройка обеспечивает пользователей необходимостью одновременно нажимать кнопки CTRL, ALT и DEL каждый раз при входе в ОС, что делает процедуру входа более защищенной.

Отключите возможность отображения имени пользователя (в поле **«Пользователь»**), выполнившего последним вход в систему, воспользовавшись соответствующей политикой безопасности **«Интерактивный вход в систему: не отображать последнего имени пользователя»**. Данная политика исключает возможность несанкционированного манипулирования именем пользователя в сети.

Концепция **«безопасного входа в систему»** реализована полностью.

5. С целью уведомления пользователей локальной сети включите возможность отображения текста сообщения следующего содержания: **«ВНИМАНИЕ!!! Вы входите в корпоративную сеть компании. Причинение вреда аппаратно-программному обеспечению компании преследуется в административном порядке. Будьте аккуратны, это Ваше имущество!!!»**, воспользовавшись локальными политиками **«Интерактивный вход в систему: заголовок сообщения для пользователей при входе в систему»** и **«Интерактивный вход в систему: текст сообщения для пользователей при входе в систему»**.

6. Практический смысл следующего задания заключается в активации так называемой модели «гостевого доступа», позволяющей организовать беспрепятственный общий доступ к объектам (файлам и каталогам) файловой системы из локальной сети. Эта модель является оптимальным выбором для домашнего применения, хотя обладает ослабленной безопасностью в процессе эксплуатации. В этой связи, критически необходимо использовать дополнительные аппаратно-программные средства для защиты клиентских компьютеров от несанкционированного доступа, вирусов и внешних атак.

Кроме модели «гостевого доступа», существует еще одна, классическая модель доступа, называемая «обычной», имеющая место при организации общих сетевых ресурсов. Модель «обычного доступа» обладает повышенным уровнем

безопасности и гибкостью при настройке прав. Поэтому применение данной модели целесообразно в корпоративных условиях.

Чтобы активировать модель «гостевого доступа», во-первых, необходимо включить встроенную учетную запись «Гость». Для этого следует найти политику безопасности **«Учетные записи: Состояние учетной записи «Гость»** и перевести соответствующий системный параметр безопасности в положение **«Включено»**.

Во-вторых, в локальной политике **«Сетевой доступ: модель совместного доступа и безопасности для локальных учетных записей»** следует изменить значение параметра модели совместного доступа в положение **«Гостевая – локальные пользователи удостоверяются как гости»**.

В-третьих, в локальной политике **«Учетные записи: ограничить использование пустых паролей только для консольного входа»**, регламентирующей использование пустых паролей, необходимо перевести параметр безопасности в состояние **«Отключено»**. Это позволит пользователям с учетной записью **«Гость»** и пустым паролем иметь возможность беспрепятственного доступа в систему из локальной сети. По умолчанию, во включенном состоянии этого параметра, использование пустых паролей допускается только для консольного входа, то есть для входа в систему с клавиатуры компьютера.

Очевидно, что данная политика в состоянии **«Отключено»** также ослабляет системную безопасность настраиваемой среды при доступе к так называемым «административным» ресурсам, если учетные записи последних надежно не защищены парольной защитой.

Наконец, следует проверить наличие пользователя «Гость» в числе тех, кому в принципе разрешен доступ из локальной сети. Для этого откройте изученную ранее (**секция В** текущего задания) ветвь **«Параметры безопасности | Локальные политики | Назначение прав пользователя»** и в локальной политике **«Отказ в доступе к компьютеру из сети»** убедитесь в отсутствии учетной записи «Гость» среди запрещенных. Если пользователю «Гость» доступ из сети запрещен, то удалите учетную запись.

Таким образом, последние четыре политики позволяют организовать «гостевой доступ» из локальной сети к тому компьютеру, на котором данные настройки были применены. Как следствие, реализованная конфигурация при

использовании на каждом локальном узле в рабочей группе или домене обеспечивает беспрепятственный взаимный доступ к общим локальным ресурсам.

8. Сохраните и закройте консоль администрирования MMC.

При выполнении заданий секции используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– выйдите из системы, снова войдите в нее и проверьте влияние новых значений системных параметров политик безопасности,

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №6.2. Изучение основных возможностей программного средства **«Шаблоны безопасности»** в среде ОС Windows XP на конкретных примерах.

В предыдущих заданиях практической работы были рассмотрены отдельные политики безопасности и принадлежащие им системные параметры, изменяемые при конфигурировании безопасности ОС. Однако гораздо эффективней конфигурировать ОС в процессе ее загрузки посредством единовременного применения группы параметров безопасности. Для этих целей в среде ОС Windows XP существует специализированное программное средство **«Шаблоны безопасности»**, представляющее собой оснастку, как и прежде добавляемую к дереву консоли администрирования MMC. В рамках данной оснастки имеется возможность создавать и применять в системе текстовые файлы, содержащие в себе все необходимые настройки безопасности для безопасных областей, поддерживаемых локальной политикой. Именно данные текстовые файлы в ОС принято называть шаблонами безопасности. В ОС Windows XP существует ряд штатных шаблонов безопасности, определяющих конфигурацию безопасности по семи категориям:

1) Политики учетных записей – это набор параметров аутентификации учетных записей. Для учетных записей домена параметры учетной политики должны быть одинаковы по всему домену. Данные политики подразделяются на:

– *Политика паролей* – ограничения на пароль, его минимальную длину, хранение старых паролей, минимальный и максимальный срок действия пароля, сложность пароля и, возможно, обратимое шифрование хранимых данных.

– *Политика блокировки учетной записи* отвечает за действие, которое должно выполняться при вводе неверного пароля, включая пороговое число неудачных попыток входа в ОС, при котором происходит блокировка учетной записи или ответные действия, включая частоту сброса счетчиков попыток входа.

– *Политика Kerberos* – набор параметров протокола сетевой аутентификации Kerberos v.5, в частности, включающего время жизни для билетов на их выдачу, билетов службы, максимальное расхождение часов и проверку членства в группе и статуса блокировки учетных записей.

2) Локальные политики – параметры безопасности только для компьютера, на котором применяется шаблон безопасности. Они применяются к базе данных учетной записи локального узла и делятся на три категории.

– *Политика аудита* – набор отслеживаемых событий, которые будут храниться в журнале безопасности локального компьютера.

– *Назначение прав пользователя* определяет участников безопасности, которым будут даны права пользователей на локальном компьютере. Эти права приоритетнее любых разрешений ФС NTFS, назначенных объекту (файлу или каталогу).

– *Параметры безопасности* – спектр параметров, заданных в Реестре ОС. Обычно они указывают, отображать ли имя последнего пользователя, под которым входили в компьютер, или изменять ли имя учетной записи «Администратор».

3) Журнал событий – набор свойств журналов приложений, безопасности и системы, включая максимальный размер журнала, пользователей, которые могут его просматривать, срок хранения событий в журналах и действия, которые надо предпринять, если журналы безопасности достигли заданного максимального размера.

4) Группы с ограниченным доступом позволяют зафиксировать членство в группах безопасности. Допустимые группы безопасности выбирает создатель шаблонов безопасности. Обычно в эту группу включаются «Опытные пользователи», «Администраторы предприятия» и «Администраторы схемы». В результате можно явно указать, какие участники безопасности могут быть членами группы с

ограниченным доступом. Данная политика также определяет, членом каких групп может быть сама группа с ограниченным доступом.

5) Системные службы позволяют задать ограничения для служб, установленных на компьютере, в том числе их статус (активизирована или отключена) и какие участники вправе ее запустить или остановить. В частности, например, можно настроить данную политику таким образом, чтобы была отключена служба **«Routing and Remote Access»** (**«Маршрутизация и удаленный доступ»**) на всех клиентских рабочих станциях. Это обеспечит запрет пользователям настраивать свои персональные компьютеры в качестве серверов удаленного доступа.

6) Реестр определяет безопасность разделов Реестра ОС и их кустов: какие участники безопасности вправе изменять параметры безопасности и аудит каких действий по модификации Реестра следует вести.

7) Файловая система определяет параметры избирательного списка управления доступом (DACL) и системного списка управления доступом (SACL) для любых каталогов, включенных в эту политику. Эти каталоги должны располагаться на носителе с ФС NTFS.

Известно, что компьютеры в сети могут выступать в разных ролях, то есть иметь различное назначение. Это обстоятельство влияет на выработку решения по тому, какие параметры следует применять для формирования политики безопасности для того или иного узла. Это приводит к тому, что перед определением шаблонов безопасности необходимо выявить компьютеры в сети, для которых нужно создать одинаковые параметры безопасности. Обычно для этого достаточно определить роль, которую каждый компьютер выполняет в сети, и уникальные требования безопасности для каждой роли.

Каждая роль, в конечном итоге, будет связана с шаблоном безопасности, определяющим типовую или требуемую безопасность для этого класса компьютеров. Наиболее распространенные роли компьютеров в сети следующие.

Контроллеры домена хранят базу данных Active Directory, требования безопасности для защиты которой являются самыми строгими.

Серверы приложений содержат клиентские серверные приложения, например, Web-приложения, базы данных SQL или почтовые серверные приложения. В каждой из указанных выше категорий можно определить соответствующие параметры безопасности для серверного приложения.

Файловые серверы хранят данные, совместно используемые в сети. В рамках определения безопасности можно создать специальные списки DACL для определенных хранилищ данных.

Серверы печати предназначены для организации печати на принтерах, находящихся в общем доступе для компьютеров локальной сети. Для каждого сетевого принтера могут быть установлены различные права доступа для разных пользователей.

Серверы экстрасети – компьютеры с любой сетевой ОС, не являющиеся членами Active Directory. Хотя они могут проводить аутентификацию, но, как правило, располагаются в нейтральной (демилитаризованной DMZ-зоне) и имеют ограниченный доступ к ресурсам внутренней локальной сети.

Рабочие станции – клиентские компьютеры с сетевой ОС, не покидающие территориально офис предприятия. Их можно подразделять в зависимости от отдела или филиала, где они установлены.

Портативные компьютеры – клиентские узлы, имеющие возможность мобильного перемещения. Пользователи этих компьютеров могут обладать особыми привилегиями для выполнения некоторых задач вне корпоративной локальной сети.

Киоски устанавливаются в общественных местах и выполняют одно общедоступное приложение. В шаблоне безопасности киоска можно настроить автоматическую регистрацию на входе с использованием предварительно созданной учетной записи, позволяющей работать со специализированным инсталлированным приложением.

Нетрудно заметить, что такое структурирование узлов по ролям способствует выработке решения по разделению параметров безопасности на группы для их дальнейшей интеграции в соответствующие шаблоны безопасности. Анализ безопасности, выработка решений с подбором соответствующих параметров безопасности, а также примеры реального внедрения принятых решений подробно описываются в практическом курсе MCSE по безопасности сети от корпорации Microsoft.

В рамках настоящей практической работы для ознакомления с базовыми возможностями рассматриваемого программного средства **«Шаблоны безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Шаблоны безопасности»** способом, изученным ранее, и разверните ее, чтобы были видны все ее элементы.

3. Создайте новый шаблон безопасности. Для этого выберите манипулятором мышь строку **«C:\WINDOWS\security\templates»**, показывающую локальное место хранения шаблонов безопасности в системе, и далее команду **«Создать шаблон…»** либо из выпадающего контекстного меню, либо из меню **«Действие»** на панели инструментов.

4. Откройте только что созданный шаблон безопасности и обратите внимание на то, что он включает в себя все семь категорий, описанных выше. Кроме того, просмотрите содержащиеся в нем политики безопасности и убедитесь, что все они находятся в состоянии **«Не определено»**.

Таким образом, создается пустой шаблон безопасности, в который можно внести все необходимые параметры, относящиеся к организуемой политике безопасности.

5. Сохраните созданный шаблон, открыв контекстное меню **«Действие»** и выбрав команду **«Сохранить как…»**. Имя шаблону присвойте, например, **MyFirstShablon** или определите его самостоятельно.

Как утверждалось ранее, ОС Windows XP изначально включает в себя ряд шаблонов безопасности, которые могут быть взяты в качестве основы для построения собственной политики безопасности. В частности, в распоряжении администратора может быть готовая политика безопасности, которая, в свою очередь, может быть улучшена и применена позже в системе.

По степени безопасности существуют четыре типа шаблонов:

- основной (Basic),
- безопасный (Secure),
- высокой степени безопасности (High secure),
- смешанный (Miscellaneous).

В качестве примера, среди штатных шаблонов безопасности находятся такие, как **Hisecdc** (сокр. **High secure domain controller**), который устанавливает самый высокий уровень безопасности для контроллера домена, или **Securews** (сокр. **Secure work station**) – устанавливает средний уровень безопасности для рабочих станций.

Любой из доступных шаблонов может быть использован для разработки собственной политики безопасности.

Внимание! Перед модификацией штатного шаблона безопасности его следует предварительно сохранить под другим именем, чтобы он не был испорчен перезаписью.

6. Для создания шаблона безопасности, обладающего стандартной функциональностью, возьмите за основу системный шаблон **Setup security**, обеспечивающий уровень безопасности по умолчанию, и сохраните его с другим именем, выбранным самостоятельно или, например, **MySecondShablon**.

7. В только что сохраненном шаблоне выберите самостоятельно и измените несколько политик безопасности. При необходимости воспользуйтесь теми системными политиками, которые уже изменялись в предыдущих заданиях, например, при организации модели «гостевого доступа». Сохраните сконфигурированный таким образом шаблон безопасности.

8. Примените созданный шаблон безопасности в системе. Для этого в оснастке **«Политика «Локальный компьютер»** щелкните дважды на разделе **«Конфигурация компьютера»** и разверните подраздел **«Конфигурация Windows»**. Щелкните правой кнопкой мыши по строке **«Параметры безопасности»**, а затем – по команде **«Импорт политики»**. Выберите созданный шаблон безопасности и импортируйте его в систему, нажав **ОК**.

Примечание. Для возврата системных параметров безопасности в состояние **«по умолчанию»** примените в системе штатный, неизмененный шаблон безопасности **Setup security**. Уровень безопасности ОС Windows XP будет приведен к начальному состоянию.

9. Сохраните и закройте консоль администрирования MMC.

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– перезагрузите компьютер и проверьте влияние новых значений системных параметров политик безопасности,

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №6.3. Изучение основных возможностей программного средства **«Анализ и настройка безопасности»** в среде ОС Windows XP на конкретных примерах.

Другим, не менее важным, штатным программным средством, предназначенным для анализа настроек некоторого шаблона безопасности и сравнения их с текущими настройками безопасности действующего в системе шаблона, является оснастка **«Анализ и настройка безопасности»**. Учитывая то, что в ОС Windows XP имеется огромное количество политик безопасности, отслеживать каждую из них по отдельности представляется проблематичным. Однако анализ безопасности системы посредством рассматриваемого инструмента позволяет обнаруживать «дыры» в системе, тестировать влияние группового изменения настроек безопасности в ОС без их непосредственного применения, а также выявлять любые отклонения в политике безопасности сети.

Для ознакомления с базовыми возможностями изучаемого инструмента **«Анализ и настройка безопасности»** в среде ОС Windows XP выполните следующее:

1. Разверните окно созданной ранее консоли администрирования MMC, если оно находится в свернутом состоянии на панели задач, или загрузите консоль снова.

2. Добавьте в корень дерева консоли MMC новую оснастку **«Анализ и настройка безопасности»** способом, изученным ранее, и выберите ее.

После этого шага инструмент **«Анализ и настройка безопасности»** будет доступен, но нефункционален. Для получения необходимой функциональности его предстоит предварительно сконфигурировать.

3. Поскольку работа данного инструмента основана на использовании базы данных, сначала ее необходимо создать. Инструмент позволяет создать базу данных конфигураций и анализа безопасности, также называемую локальной базой данных политики компьютера.

В идеальном случае, база данных должна создаваться сразу же после инсталляции ОС. В этих условиях в ней будут содержаться настройки параметров безопасности в состоянии «по умолчанию». Поэтому при необходимости данная база может быть экспортирована сразу после загрузки системы и быть всегда доступной на случай «отката» к первоначальным настройкам.

Создайте новую базу данных. Для этого в меню **«Действие»** выберите команду **«Открыть базу данных...»**, введите в появившемся диалоговом окне новое

имя базы данных (имя выберите самостоятельно) и щелкните на кнопке **«Открыть»**. В следующем окне выберите созданный ранее шаблон безопасности с именем **MyFirstShablon** и импортируйте его в базу данных, подтвердив намерение командой **«Открыть»**.

Если все сделано без ошибок, то при выборе оснастки **«Анализ и настройка безопасности»** в верхней части области сведений консоли администрирования MMC будет отображаться системный путь, где хранится только что созданная база данных системы безопасности ОС Windows XP.

4. Для анализа сформированной базы данных необходимо выбрать манипулятором мышь оснастку **«Анализ и настройка безопасности»**, а затем – команду **«Анализ компьютера…»** в контекстном меню **«Действие»** (альтернативным способом данную команду можно выбрать из выпадающего контекстного меню, если щелкнуть правой кнопкой мыши по выбранной оснастке). В появившемся диалоговом окне обратите внимание на системный путь и имя файла журнала ошибок, в котором будут сохраняться результаты анализа. При необходимости путь по умолчанию и имя файла могут быть заменены на более подходящие для организации удобного доступа.

Нажмите **ОК** для подтверждения операции анализа безопасности. В процессе проверки безопасности системы в окне состояния будет отображаться ход выполнения задания. По окончании анализа результаты отображаются справа, в области сведений, и появляется возможность просмотра и изменения необходимых настроек политик безопасности.

Если необходимо, просмотр файла журнала ошибок может быть осуществлен посредством выбора соответствующей команды **«Показать файл журнала»** в меню **«Действие»** на панели инструментов.

5. Последовательно проанализируйте параметры безопасности двух разделов **«Политики паролей»** и **«Локальные политики»**, щелкнув манипулятором мышь по каждому из включенных подразделов. Обратите внимание, что в области сведений справа отображаются теперь три колонки с названиями **«Политика»**, **«Параметр базы данных»** и **«Параметр компьютера»**, то есть имеется возможность сравнения действующих в системе и настраиваемых системных параметров политик безопасности.

6. Измените в базе данных несколько выбранных самостоятельно параметров безопасности анализируемых политик. Для этого щелкните манипулятором мышь

на выбранной политике и измените системное значение параметра в появившемся диалоговом окне **«Свойства»**, предварительно установив флажок **«Определить следующую политику в базе данных»**. Описание сущности изменяемого параметра безопасности доступно на соответствующей вкладке **«Объяснение параметра»** окна **«Свойства»**.

Внимание! Имейте ввиду, что изменяемые системные параметры влияют только на базу данных, а не на текущие параметры компьютера.

Таким образом, сравнивая текущие параметры действующей в системе политики безопасности можно настроить необходимые системные параметры с целью их экспортирования в новый шаблон безопасности и дальнейшего использования в ОС Windows XP.

7. Экспортируйте базу данных только что измененных параметров в новый шаблон безопасности с именем **MyThirdShablon**. Сохраните консоль ММС, выгрузите и загрузите ее снова. Проверьте наличие шаблона **MyThirdShablon** в оснастке **«Шаблоны безопасности»** и действительность изменения выбранных параметров политик безопасности внутри шаблона.

Таким образом, созданный шаблон безопасности теперь может быть, при необходимости, применен в системе способом, изученным в предыдущем задании практической работы.

8. Закройте консоль администрирования ММС, сохранив ее.

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №6.4. Изучение основных возможностей программного средства **«Брандмауэр подключения к Интернету»** в среде ОС Windows XP на конкретных примерах.

Теперь, когда основные действия по предотвращению несанкционированного локального проникновения определены, необходимо обеспечить дополнительный уровень защиты от потенциальных атак извне. Одним самых важных, штатных компонентов защиты ОС Windows XP от внешних угроз является инструмент, ограничивающий обмен информацией между локальной средой и сетью Интернет, **«Брандмауэр подключения к Интернету»** (Internet Connection Firewall, **ICF**), коротко брандмауэр или сетевой экран.

ICF представляет собой достаточно мощную систему защиты, которая отслеживает все аспекты работы линий связи и проверяет исходные и конечные адреса информационных пакетов. Для предотвращения попадания нежелательного трафика в локальную сеть из Интернета **ICF** содержит список всех соединений контролируемого компьютера, располагающихся в специальной таблице. Входящий трафик сравнивается с данными из этой таблицы и при несовпадении входящие пакеты блокируются. В частности, это препятствует атакам в виде сканирования портов из сети Интернет. При этом стоит помнить, что **ICF** блокирует любой пакет, неожиданно приходящий в локальную сеть, включая те, которые могут быть полезны пользователю, например, пакеты электронной почты. Поэтому **ICF** необходимо сконфигурировать таким образом, чтобы исключить подобные коллизии и пропускать сообщения, направляя их соответствующему адресату.

Для ознакомления с базовыми возможностями брандмауэра ICF в среде ОС Windows XP выполните следующее:

1. Включите **ICF** в среде ОС Windows XP. Для этого необходимо выбрать сетевое подключение (**«Пуск | Панель управления | Сетевые подключения»**), предполагаемое к защите посредством **ICF**. Затем, либо из контекстного меню выбрать команду **«Свойства»**, либо щелкнуть по команде **«Изменение настроек подключения»** слева в группе команд **«Сетевые задачи»**. В окне **«Свойства сетевого подключения»** на вкладке **«Дополнительно»** необходимо щелкнуть по кнопке **«Параметры»** брандмауэра Windows и закрыть несанкционированный

доступ из сети, выбрав **«Включить (рекомендуется)»** на появившейся вкладке **«Общие»**.

2. Для обеспечения контроля за действиями **ICF** в системе предусмотрен механизм ведения журнала безопасности, который позволяет создавать список действий системы защиты, а именно установку запрета или разрешения на трафик со стороны **ICF**. Это бывает весьма полезно при организации безопасной среды. Включение процесса документирования за действиями **ICF** осуществляется на вкладке **«Дополнительно»** брандмауэра Windows. Для этого необходимо щелкнуть по кнопке **«Параметры»** в разделе **«Ведение журнала безопасности»**, поставить опциональные флажки напротив **«Записывать пропущенные пакеты»** и **«Записывать успешные подключения»**. Подтвердите операцию, нажав **ОК**.

Кроме того, имеется возможность регулировать дополнительную функциональность по протоколу управляющих сообщений Интернета ICPM (в частности, позволяющего компьютерам в сети обмениваться информацией об ошибках). Список запросов из сети Интернет, на которые будет отвечать конфигурируемый компьютер, представлен в виде набора параметров в разделе **«Протокол ICMP»** на вкладке **«Дополнительно»**.

Включите протоколирование следующих сообщений:

- входящих эхо-запросов;
- входящих меток времени;
- входящих запросов маршрутизатора;
- переадресацию.

Уместно отметить, что по своей сути журнал **ICF** является программным средством, также предназначенным для аудита системы безопасности наряду с теми, которые изучаются в соответствующей практической работе. К числу подобных средств также следует отнести автономную оснастку **«Просмотр событий»**, расширение **«Политика аудита»** в рамках оснастки **«Политика «Локальный компьютер»**, а также рассмотренную в предыдущем задании оснастку **«Анализ и настройка безопасности»**.

В частности, посредством расширения **«Политика аудита»** можно осуществлять проверку и регистрацию событий в следующих категориях:

- управление учетной записью,
- ввод-вывод данных в сети,
- доступ к конкретному объекту (файлу или каталогу),

- изменение политик сети,
- попытки использования специальных привилегий,
- загрузка пользовательских процессов,
- другие системные действия.

Поскольку аудит в значительной степени расходует системные ресурсы, необходимо заранее определиться с элементами, требующими контроля (иными словами, надо четко представлять себе, что необходимо контролировать, чтобы излишне не нагружать систему).

3. Журнал **ICF** имеет свой уникальный формат. В заголовке указываются версия используемого межсетевого экрана **ICF**, имя журнала безопасности, примечание о том, что вход в систему регистрируется по локальному времени, и список доступных полей для регистрационных записей (табл. 6.2).

Польза журнала безопасности **ICF** состоит в том, что после его просмотра можно обнаружить попытки несанкционированного доступа к сети. Изучив поля **action**, **scr-ip** и **dst-ip**, в частности, можно определить, пытается ли кто-то повредить сеть в целом или вывести из строя какое-то определенное устройство.

В любой текстовый редактор загрузите журнал безопасности **ICF**, располагающийся в системном каталоге **C:\Windows\pfirewall.log** и найдите все его отмеченные атрибуты, поля и изучите содержимое журнала в целом, воспользовавшись таблицей 6.2. Вероятно, может оказаться, что осуществленных записей в журнале ICF будет не слишком много – это связано с тем, что журнал безопасности был активирован сравнительно недавно.

Дополнительно журнал безопасности ICF может быть переименован и сохранен в место, путь к которому системный администратор определяет самостоятельно. Это удобно в том случае, когда имеется необходимость вести несколько отчетов, например, по дням недели или времени дня. Размер файла журнала безопасности ICF может быть изменен на вкладке **«Параметры журнала»** с установленного в 4Мб по умолчанию до 32Мб по необходимости.

Таблица 6.2. Поля ввода данных в журнале безопасности **ICF**

№ п/п.	Поле журнала безопас-ности ICF	Описание поля
1.	**Action**	Операция, перехваченная брандмауэром Windows. Входящие данные включают в себя: **OPEN**, **CLOSE**, **DROP**, **INFO-EVENTS-LOST** (указывается количество произошедших событий, не сохраненных в журнале).
2.	**Date**	Дата ввода файла в формате **YY-MM-DD** (год-месяц-день).
3.	**Dst-ip**	**IP**-адрес конечного пункта доставки пакета.
4.	**Dst-port**	Номер порта конечного пункта доставки пакета.
5.	**Icmpcode**	Число, обозначающее поле кода в **ICMP**-сообщении.
6.	**Icmptype**	Число, обозначающее поле ввода текста в **ICMP**-сообщении.
7.	**Info**	Поле для ввода информации о событии, которое зависит от типа действия.
8.	**Protocol**	Протокол связи. Если это не **TCP**, **UDP** или **ICMP**, то здесь указывается цифра.
9.	**Size**	Размер пакета (байт).
10.	**Scr-ip**	**IP**-адрес устройства-отправителя.
11.	**Scr-port**	Номер порта отправителя.
12.	**Tcpack**	**TCP**-номер подтверждения пакета.
13.	**tcp-flags**	**TCP**-флаг, указываемый в начале пакета: **A** – Ack (важность поля подтверждения), **F** – Fin (последний пакет), **P** – Psh (функция «проталкивания» пакета), **S** – Syn (синхронизация последовательности номеров), **U** – Urg (важность поля указателя срочности).
14.	**Tcpsyn**	**TCP**-последовательность номеров пакетов.
15.	**Tcpwin**	**TCP**-размер окна (байт).
16.	**Time**	Время регистрации файла в формате **HH:MM:SS** (часы:минуты:секунды).

4. Иногда в процессе работы возникает необходимость не контролировать брандмауэром ICF трафик, проходящий в сети через доверенные специализированные приложения, например, приложения контроля информационных пакетов, торрент-клиенты или трафик, проходящий через

определенные открытые порты, например, настроенные под так называемый «портфорвардинг». Для этих целей в **ICF** предусмотрена возможность исключений.

Для активации данной возможности по отношению к программам на вкладке **«Исключения»** брандмауэра Windows добавьте, для примера, выбранное приложение, генерируемый трафик которого не будет контролироваться впредь. Закройте окно **«Добавление программы»** и обратите внимание на то, что только что выбранная программа появилась в области исключений **«Программы и службы»** на исследуемой вкладке (напротив неконтролируемого приложения стоит флажок активации, снятие которого обратно приводит к контролю трафика этого приложения).

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Изученные в первом задании практической работы инструменты и возможности не являются исчерпывающими для всеобъемлющей организации сетевой безопасности в ОС (спектр специализированных программных средств, предназначенных для локальной и сетевой защиты компьютера, достаточно широк, а его детальное рассмотрение в практикуме не представляется возможным), однако в первом приближении они позволяют обезопасить локальную рабочую среду и в некоторой степени защитить ее от сетевого проникновения извне.

7. Работа с оснасткой "Системный монитор".Работа с модулями Tasklist и Taskkill. Настройка прав доступа к файлам с использованием командной строки.

Цель работы: продолжить изучение модулей, предназначенных для мониторинга, управления производительностью операционной системы и безопасностью, включая работу с ними с помощью средств командной строки.

7.1. Подготовка к выполнению практической работы

В предыдущих практических работах был изучен целый ряд модулей и оснасток, предназначенных для мониторинга, управления производительностью и безопасностью системы. Настоящая работа будет посвящена дальнейшему изучению настройки производительности и системы безопасности. Дополнительный акцент будет сделан на использовании функционала командной строки для доступа к указанным модулям.

I. Контроль производительности

Как известно, для того чтобы ваш компьютер и установленная на него операционная система нормально функционировали, необходимо периодически следить за ошибками и предупреждениями в журнале событий, а также проверять отчет о неполадках при помощи журнала стабильности. Но во время использования специализированных программ, игровых приложений или при работе операционной системы в целом, вы можете ощущать, что ваша система «тормозит» и работает совсем не так, как вам бы этого хотелось. Но иногда неполадки обнаруживаются не сразу, и для их идентификации требуется дополнительный анализ. Если вы не обнаружили никаких ошибок в указанных выше средствах диагностики неполадок операционной системы, то, возможно, у вас есть некие проблемы, связанные с производительностью. По определению, **производительность** – это скорость, с которой компьютер выполняет системные задачи и задачи установленных и используемых приложений. Общая производительность системы может быть ограничена скоростью доступа к физическим жестким дискам, количеством памяти доступной текущим процессам, скоростью процессора и максимальной пропускной способностью сетевых интерфейсов. Иногда, именно при помощи компонентов, предназначенных для мониторинга производительности вашего компьютера, вы можете проанализировать и отследить использование доступных ресурсов

отдельными приложениями и процессами, после чего правильно спланировать аппаратные ресурсы в соответствии с возрастающими запросами.

Для обнаружения проблем с производительностью системы используется утилита **«Системный монитор»**. Системный монитор – это оснастка консоли управления MMC операционных систем Windows, предназначенная для анализа работы программ на производительность компьютера в реальном времени. Помимо вышеперечисленных действий, при помощи данной оснастки вы можете в реальном времени осуществлять контроль над производительностью приложений и оборудования, выбирать данные, которые будут сохраняться в файлах журналов, задавать пороговые значения для оповещений и автоматических действий, генерировать отчеты и просматривать историю производительности системы, используя различные способы сортировки и многое другое. Данное средство удобно для кратковременного наблюдения за текущей производительностью локального или удаленного компьютера. Например, если требуется проследить за выполнением какого-либо системного процесса.

Системный монитор визуально отображает встроенные счетчики производительности Windows в реальном времени или в режиме просмотра предыдущих дат, а также совмещает службу журналов и оповещения производительности (Performance Logs and Alerts – PLA: служба, которая по заранее определенному графику собирает данные о производительности на локальном и удаленных компьютерах, а затем заносит их в журнал или использует для создания сообщения) и системный монитор.

В этой работе вы узнаете о том, как открывать и использовать оснастку **«Системный монитор»** и познакомитесь со средствами узла **«Средства наблюдения»**, а также с различными счетчиками.

Секция А. Оснастка «Системный монитор»

Как говорилось выше, **«Системный монитор»** – это оснастка, поддерживающая несколько графических представлений, позволяющих визуально оценить данные журналов производительности. Открыть данную оснастку вы можете несколькими способами:

– Нажмите на кнопку **«Пуск»** для открытия меню, откройте **«Панель управления»**, из списка компонентов панели управления выберите категорию

«Производительность и обслуживание», выберите подкатегорию **«Администрирование»**, а затем перейдите по ссылке **«Производительность»**;

– Воспользуйтесь комбинацией клавиш +R для открытия диалога **«Выполнить»**. В диалоговом окне **«Выполнить»**, в поле **«Открыть»** введите *perfmon.msc* и нажмите на кнопку **«ОК»**;

Откройте **«Консоль управления ММС»**. Для этого нажмите на кнопку **«Пуск»**, в поле поиска введите *mmc*, а затем нажмите на кнопку **«Enter»**. Откроется пустая консоль ММС. В меню **«Консоль»** выберите команду **«Добавить или удалить оснастку»** или воспользуйтесь комбинацией клавиш **Ctrl+M**. В диалоге **«Добавление и удаление оснасток»** выберите оснастку **«Элемент ActiveX»** и нажмите на кнопку **«Добавить»**. В открывшемся мастере нажмите **"Далее"**, выберите в списке **"Категория элемента"** пункт **"Все категории"** и тип элемента **"System Monitor Control"**. Кроме того, необходимо подключить оснастку **"Журналы и оповещения производительности"**.

Стоит обратить внимание на то, что не все пользователи могут использовать весь функционал данной оснастки. Пользователи, которые входят в состав группы **«Администраторы»** имеют полные права и могут пользоваться всеми функциональными возможностями оснастки **«Системный монитор»**. Обычные пользователи могут только открывать журналы для просмотра в мониторе производительности, а также изменять свойства отображения монитором производительности данных истории во время просмотра.

Настройка системного монитора

Системный монитор содержит в себе богатейший функционал и, соответственно, имеет множество настроек для наилучшего отображения данных. Рассмотрим настройки данного средства. Открыть диалоговое окно настроек системного монитора вы можете одним из следующих способов:

– Нажмите правой кнопкой мыши на области сведений с графиком производительности и из контекстного меню выберите команду **«Свойства»**.

– Выбрав в левом окне пункт "Системный монитор", нажмите левой кнопкой мыши один из значков, расположенных над окном графиков (четвертый справа).

– Щелкнув левой кнопкой мыши на окно графика, нажмите комбинацию клавиш CTRL+Q.

Диалоговое окно свойств системного монитора состоит из пяти вкладок. Рассмотрим каждую вкладку отдельно.

Вкладка «Общие» свойств системного монитора

На вкладке **«Общие»** вы можете указать настройки, которые будут применены для узла **«Системный монитор»**. Вы можете изменить следующие настройки:

– **Вид.** Мы можете установить, какой вид примет окно графика – график, гистограмма или отчет.

– **Отображаемые элементы**. При помощи этой группы вы можете отображать или скрывать ключевые элементы, которые расположены в узле **«Системный монитор»**. Флажок **«Легенда»** отвечает за отображение легенды внизу области сведений. Если снять флажок **«Строка значений»**, то значения, которые находятся под диаграммой, не будут отображаться. Флажок **«Панель инструментов»** отвечает за отображение панели инструментов, расположенной над диаграммой;

– **Данные отчета и гистограммы**. Системный монитор поддерживает выборку данных вручную, по требованию и в автоматическом режиме с заданным интервалом; эта функция применима только к данным в реальном масштабе времени. В режимах гистограммы и отчета при выборе среднего, минимального или максимального значения отображаемые данные пересчитываются после очередной выборки. Это приводит к дополнительной нагрузке на систему;

– **Автоматический съем показаний**. Данная опция (включена, если установлена галочка "Снимать показания каждые ___ сек") позволяет осуществлять автоматическую выборку данных. Снятие показаний счетчиков в режиме выборки данных вручную выполняется кнопкой **«Обновить данные»**, которая находится на панели инструментов или при помощи комбинации клавиш **Ctrl+U**. Изменить ручной режим выбора данных на автоматический также можно при помощи кнопки **«Разрешить изменять отображение»**, расположенной на панели инструментов, или комбинацией клавиш **Ctrl+F**;

– Раскрывающийся список **"Представление"** позволяет выбрать объемное или плоское оформление окна системного монитора.

– Раскрывающийся список **«Рамка»** позволяет вам добавить или убрать обрамление для диаграммы.

– **Элементы диаграммы**. Элементы этой группы позволяют изменять параметры выборки данных. Для автоматической выборки данных через определенные промежутки времени, введите в текстовое поле **«Съем показаний каждые:»** значение интервала измеряется в секундах. По умолчанию этот интервал равен 1 секунде. В текстовом поле **«Длительность»** вы можете указать время в секундах, через которое самые ранние данные будут заменяться новыми. Обновление данных каждые 15 секунд оправдано, только в том случае, когда планируется вести наблюдение не больше четырех часов. Если следует вести наблюдение восемь часов и более, задавайте интервал обновления более 300 секунд (5 минут). Постоянное наблюдение за активностью следует осуществлять с интервалом не менее 15 минут.

Вкладка «Источник» свойств системного монитора

Эта вкладка предназначена для выбора источника отображения для просмотра текущих собираемых данных. Установив переключатель на опции **«Текущая активность»**, системный монитор будет показывать изменения в производительности, согласно установленным вами счетчикам. Кроме текущей активности вы также можете указать путь к сохраненному ранее файлу журнала. Для этого установите переключатель в положение **«Файлы журнала»**, а затем добавьте файлы, которые следует использовать в качестве источника данных. Журналы также можно использовать для анализа тенденций и планирования распределения ресурсов. Помимо указанных выше источников, вы также можете записывать и извлекать данные о производительности в базы данных SQL. Сведения, находящиеся в базе данных, можно извлекать запросами и включать в отчеты. Основным требованием для использования данного источника является наличие SQL сервера баз данных.

Вкладка «Данные» свойств системного монитора

Вкладка **«Данные»** свойств системного монитора позволяет вам настраивать отображение выводимых данных. В поле **«Счетчики»** вы можете просмотреть все счетчики, добавленные для анализа производительности. Используя данную вкладку, устанавливаются следующие параметры:

– **Добавить**. Данная функция позволяет добавлять дополнительные счетчики при помощи диалогового окна **«Добавить счетчики»**;

– **Удалить**. Нажав на эту кнопку счетчик, который выделен в списке, будет удален;

– **Цвет**. Эта опция позволяет указать цвет для выбранного счетчика;

– **Масштаб**. Текущий раскрывающийся список отвечает за масштаб отображения выбранного счетчика в режиме графика или гистограммы. Значения счетчика вы можете указать от 0,0000001 до 1000000,0. Изменение масштаба позволит вам сделать диаграмму более наглядной;

– **Ширина**. Эта опция позволяет указать ширину линии для выбранного счетчика. Изменение ширины влияет на набор доступных типов линии;

– **Стиль**. Данная опция отвечает за изменение стиля линии выбранного счетчика. Смена стиля возможна, если для линии выбрана ширина, назначенная для использования по умолчанию.

Вкладка «График» свойств системного монитора

При помощи этой вкладки свойств системного монитора вы можете изменять отображение графика в области сведений по своему вкусу. Здесь вы можете найти практически все настройки, которые можно было бы изменить в изображении графика. Рассмотрим каждый из параметров:

– **Заголовок**. Текущий параметр отвечает за название графика, которое будет отображено под панелью инструментов;

– **Вертикальная ось**. При помощи этого параметра вы можете дать название вертикальной оси координат;

– **Отображать**. Этот параметр позволяет вам отобразить вертикальную или горизонтальную сетку для графика, а также включить отображение подписей со значениями для вертикальной шкалы;

– **Диапазон значений вертикальной шкалы**. Здесь вы можете установить максимальное и минимальное значение, которое будет отображаться на графике.

Вкладка «Оформление» свойств системного монитора

На этой вкладке вы можете выбрать параметры, предназначенные для визуального оформления графика данной оснастки. В группе **«Шрифт»** вы можете изменить шрифт текста и чисел, присутствующих на диаграмме. Для того чтобы их изменить шрифт, нажмите на кнопку **«Изменить»**, а затем на вкладке **«Шрифт»** задайте такие параметры, как шрифт, начертание, размер и, при необходимости,

набор символов. На данной вкладке особый интерес может представлять группа **«Цвет»**. При помощи этой группы вы можете настроить цвета буквально для всех элементов области сведений, а именно:

- **Фоновый рисунок**. Позволяет указать цвет фона области окна, в которой отображается диаграмма;
- **Фон элемента управления**. Определяет цвет фона, окружающего область окна, в которой отображается диаграмма;
- **Текст**. Указывает цвет отображаемого на диаграмме текста;
- **Сетка**. При отображении на диаграмме сетки, этот параметр позволяет задать цвет для вертикальных и горизонтальных линий сетки.
- **Панель времени**. Данный параметр позволяет вам указать цвет для линии времени.

Секция B. Счетчики производительности – это расширяемый механизм сбора статистической информации.

Большая часть счетчиков доступна вам в оснастке **«Системный монитор»**. А некоторые счетчики устанавливаются как часть приложения стороннего производителя и их можно добавлять к группе сборщиков данных или сеансу монитора производительности. В операционных системах Windows данные о производительности поступают от используемых в компьютере компонентов или ролей серверных операционных систем. Такие данные представляются в виде объекта производительности, который обычно называется так же, как компонент, генерирующий данные. Например, объект **«Процессор»** представляет собой набор данных о производительности центрального процессора. Каждый объект производительности содержит счетчики, дающие сведения о конкретных элементах системы или службы. Например, счетчик **«% работы в пользовательском режиме»** объекта **«Процессор»** отображает средний процент времени занятости процессора по отношению ко всему времени образца. Если выбран объект на удаленном компьютере, возможна небольшая задержка, так как происходит обновление списка объектов, присутствующих на удаленном компьютере. В операционных системах Windows, для доступа к счетчикам производительности используются такие интерфейсы, как: функция RegQueryValueEx, библиотека Performance Data Helper

(PDH, предоставляемая Performance Data Helper API – Pdh.dll), инструментарий управления Windows (WMI) или ActiveX System Monitor.

В следующих разделах вы узнаете о методах добавления и удаления счетчиков производительности.

Добавление счетчиков производительности

Для выполнения мониторинга определенного объекта, вам необходимо в оснастку **«Системный монитор»** добавить конкретный счетчик. Например, операционная система Windows поддерживает несколько счетчиков, которые позволяют отслеживать процессы, выполняемые в системе. Данные этих счетчиков можно просматривать в оснастке **«Системный монитор»**. К таким счетчикам можно отнести: **Процесс: % работы в привилегированном режиме**, **Процесс: % загруженности процессора**, **Процесс: % работы в пользовательском режиме** и пр.

Для добавления счетчиков производительности, выполните следующие действия:

1. Откройте оснастку **«Системный монитор»**;
2. Выберите команду **«Добавить счетчики»** одним из следующих способов:

– Нажмите на кнопку **«Добавить»** на панели инструментов;

– Нажмите правой кнопкой мыши на области сведений с графиком производительности и из контекстного меню выберите команду **«Добавить счетчики»**.

3. В появившемся диалоговом окне **«Добавить счетчики»** вам предстоит выбрать следующее:

– В группе **«Выбрать счетчики с компьютера»** вы можете указать компьютер, за которым будет вестись наблюдение. По умолчанию выбран локальный компьютер, на котором открыта сама оснастка. По желанию вы можете указать имя компьютера, для которого вам нужно добавить счетчики производительности или ввести его IP-адрес. Также, все компьютеры, которые ранее были вами указаны, сохраняются в раскрывающемся списке данной группы;

– Как говорилось выше, для каждого счетчика производительности есть свой объект производительности, который обычно называется так же, как компонент, генерирующий данные. Комбинируя параметры выпадающего списка

"Объект" и списка **«Выбрать счетчики из списка»**, вы можете найти десятки объектов производительности;

– Группа **«Выбрать вхождения из списка»** предназначена для выбора счетчика производительности, который будет отображаться на самой диаграмме в оснастке **«Системный монитор»**. Для того чтобы выбрать указанный вами счетчик – выделите его и нажмите на кнопку **«Добавить»**, которая расположена в нижней левой части данного диалогового окна. При необходимости вы можете добавить сразу несколько счетчиков, выбрав их из списка, удерживая клавишу **CTRL**. Помимо этого вы можете добавить сразу всю группу, просто выбрав ее и установив значения **"Все счетчики"** и **"Все вхождения"**. Стоит обратить внимание на то, что элемент _Total предназначен для отображения суммы значений всех экземпляров определенного счетчика.

– По умолчанию в оснастке **«Системный монитор»** отображается счетчик **«Процессор (_Total)% загруженности процессора»**;

– Если вы сомневаетесь в назначении выбранного счетчика, то можете просмотреть его подробное описание. Для этого вам нужно нажать кнопку **«Объяснение»**, расположенную в левом нижнем углу данного диалогового окна.

4. После выбора всех требуемых счетчиков, нажмите на кнопку **«ОК»** для сохранения указанных вами счётчиков производительности.

Удаление счетчиков производительности

При проведении анализа производительности вашей системы может понадобиться удалить несколько счетчиков из получившегося отчета. Удалить счетчики можно так же просто, как и добавить. Для этого выполните одно из следующих действий:

– в области сведений оснастки **«Системный монитор»** выделите счетчик, который нужно удалить и нажмите на клавишу **DELETE**;

– откройте диалоговое окно свойств оснастки, перейдите на вкладку **«Данные»**, выберите счетчик, который для дальнейшего анализа вам больше не потребуется и нажмите на кнопку **«Удалить»**.

Секция С. Сохранение отчета о производительности

Функционал системного монитора позволяет вам экспортировать полученные отчеты для дальнейшего изучения в формат HTML и в формат с разделителями-знаками табуляции.

Для того чтобы экспортировать отчет в HTML формат, щелкните правой кнопкой мыши на области сведений и из контекстного меню выберите команду **«Сохранить параметры как»**. В появившемся диалоговом окне **«Сохранить как»** выберите папку, в которую будет сохранен отчет, в поле **«Имя файла»** введите название своего отчета. Также перед сохранением вы можете указать тип файла, содержащего отчет. По умолчанию отчет сохраняется с расширением ***.html** и его можно будет открыть в любом браузере. Причем, параметры системного монитора сохраняются в файл HTML, включая тип отображения, заголовки к диаграмме и пр. Также из раскрывающегося списка **«Тип файла»** вы можете выбрать отчет оснастки **«Системный монитор»** с расширением файла журнала с разделителями-знаками табуляции и расширением .tsv. Этот формат используется, например, для экспорта данных из журнала в электронные таблицы.

Вы можете выделить конкретный счетчик, чтобы он отображался с полужирным начертанием. Для этого выберите определенный счетчик на легенде, а затем нажмите на кнопку **«Выделить»**, которая расположена на панели инструментов. Для того чтобы снять выделения со счетчика, нажмите еще раз на кнопку **«Выделить»**, расположенную на панели инструментов оснастки.

7.2. Порядок выполнения практической работы

Задание 7.1. Контроль производительности с помощью оснастки "Системный монитор".

1. Измените настройки **"Системного монитора"** таким образом, чтобы он имел вид гистограммы.

2. Установите периодичность снятия показаний 3 секунды.

3. Обеспечьте работу "Системного монитора" с не менее чем тремя счетчиками для каждой из не менее чем 5 групп.

4. Настройте отображение горизонтальной и вертикальной сеток.

5. Отобразите название диаграммы и вертикальной оси.

6. Измените значения по умолчанию диапазона значений вертикальной шкалы.

7. Сохраните результаты работы "Системного монитора" в обоих форматах. Сравните полученный результат и наглядность каждого из форматов.

II. Модули Tasklist и Taskkill.

В предыдущей практической работе вы познакомились с функционированием модуля **"Диспетчер задач"** с использованием графического интерфейса. Существует возможность работы с ним с помощью функционала командной строки. Для этого используется команда **Tasklist**. Использование модуля **Tasklist** в командной строке позволяет осуществлять вывод данных о текущем состоянии работы процессов и служб в системе в различных форматах – в виде таблицы, в виде списка, а также в виде файла с разделителями в виде запятых. При этом в отличие от графического интерфейса, командная строка позволяет просматривать список процессов и служб, запущенных на удаленном компьютере. Кроме того, командная строка позволяет завершить одно или несколько работающих заданий или процессов. Для этого используется вторая команда – **Taskkill**. Подробную информацию о синтаксисе и использовании команд **Tasklist** и **Taskkill** можно получить из справочной системы командной строки или модуля **"Справка и поддержка"** ОС Windows XP. Ознакомьтесь с представленной в них информацией для выполнения соответствующего задания.

Задание 7.2. Управление работой заданий, процессов и служб с помощью модулей Tasklist и Taskkill.

1. Запустите консоль командной строки.

2. Осуществите запуск утилиты Tasklist. Сравните результат с результатом, полученным с помощью модуля **"Диспетчер задач"**. В чем отличие? Что кардинально отличает эти два модуля?

3. Осуществите вывод списка процессов в каждом из трех доступных форматов. Какой формат более удобный и наглядный?

4. Отсортируйте список процессов, выведенный в формате таблицы по алфавиту, а затем – в обратном порядке. Для этого самостоятельно изучите справочную систему и найдите соответствующую команду, которую необходимо использовать совместно с командой **Tasklist**. Определите самостоятельно, каким образом осуществить их совместное использование.

5. Запустите любую программу, например, блокнот. Найдите ее в списке запущенных задач в **Tasklist**. Затем завершите ее средствами утилиты **Taskkill**.

III. Работа с файлом избирательных таблиц управления доступом из командной строки.

В операционной системе Windows XP существует утилита, позволяющая осуществлять просмотр или изменение файлов избирательных таблиц управления доступом (DACL). Файлы DACL хранят сведения о разрешительных и запретительных правилах доступа к различным объектам. Таблица DACL организована таким образом, что в ней сначала записаны все запретительные правила для всех пользователей, а потом – все разрешительные. Это сделано ввиду того, что записи в таблице проверяются до первого совпадения. Поэтому сначала идет проверка запретов, а, если среди них не обнаружено записей для данного пользователя относительно конкретного объекта, то тогда уже идет проверка разрешений.

Для работы с файлом избирательных таблиц управления доступом из командной строки используется утилита **CACLS**. Вам необходимо в ходе работы изучить самостоятельно синтаксис и параметры данной утилиты с помощью справки консоли командной строки или раздела **"Справка и поддержка"** ОС Windows XP.

Задание 7.3. Управление правами доступа к объектам средствами командной строки:

1. Осуществите просмотр прав доступа на выбранный вами файл.

2. Измените права доступа для разных пользователей и групп к файлу, выбранному в предыдущем пункте задания. При этом необходимо использовать весь диапазон возможных вариантов прав доступа.

3. Повторно осуществите просмотр прав доступа на текущий файл с целью удостовериться в правильности произведенных изменений.

4. Удалите все назначенные во втором пункте задания правила доступа.

8. Управление назначенными заданиями средствами командной строки.

Цель работы: изучение работы с планировщиком заданий с использованием функционала командной строки.

8.1. Краткие теоретические сведения

«Планировщик заданий» поддерживает модель изоляции, что позволяет каждому набору задач, работающих в конкретном контексте безопасности запускаться в отдельной сессии. Механизм планировщика задач запускает переходные процессы для выполнения процессов учетных записей пользователя или компьютера для запуска триггера. **Триггер** – это набор условий, при выполнении которых запускается задание. Триггеры, основанные на времени, запускают задание однократно в определенное время суток либо ежедневно, еженедельно или ежемесячно. Триггеры, основанные на событиях, запускают задание при возникновении определенных системных событий. Задачи могут быть запущены от таких учетных записей компьютера, как LocalSystem, LocalService или NetworkService.

Задачи могут быть запущены как локально, так и удаленно. Каждая задача может содержать несколько одновременно выполняемых действий. Несколько задач могут выполняться как параллельно, так и последовательно (одна за другой), используя синхронизацию с указанной службой или событием. Каждое действие планировщика заданий записывается в журналы **«Система»** и **«Журналы приложений и служб MicrosoftWindowsTaskScheduler»**. Для работы **«Планировщик заданий»** использует несколько компонентов, которые предназначены для предоставления пользовательского интерфейса, механизма выполнения заданий, отслеживания и управления событиями, а именно:

- Оснастка консоли управления Microsoft **«taskschd.msc»**, которая включает мастер для создания и настройки задач и страницы свойств, которые обращаются к службе планировщика заданий через COM API;
- Библиотека службы планировщика заданий **SchedSvc.dll**, выполняемая внутри процесса Svchost.exe, от имени учетной записи LocalSystem, которая использует компоненты TaskSchd.dll для взаимодействия с менеджером ресурсов и компонентом Service for User, предназначенным для получения доступа к учетным

данным. Эта служба также считывает информацию о конфигурации из системного реестра и записывает задания на диск в формате XML;

– Механизм переходного процесса управления **TaskEng.exe**, который позволяет выполнять задачи от имени учетной записи пользователя и создавать пользовательские процессы, выполняющие указанные задания;

– Библиотека **TaskComp.dll**, которая обеспечивает обратную совместимость для управления и выполнения задач, которые были созданы в предыдущих версиях Windows.

Операционная система Windows предоставляет несколько средств, предназначенных для планирования заданий на локальных и удаленных компьютерах, а именно:

Запустить планировщик заданий вы можете любым из следующих способов:

– Нажмите на кнопку **«Пуск»** для открытия меню, откройте папку **«Все программы»**, затем откройте папку **«Стандартные > Служебные»** и выберите элемент **«Назначенные задания»**;

– Нажмите на кнопку **«Пуск»** для открытия меню, откройте **«Панель управления»**, из списка компонентов панели управления выберите категорию **«Производительность и обслуживание»**, а затем перейдите по ссылке **«Назначенные задания»**;

Утилита командной строки Schtasks. Утилита, которая позволяет создавать и запускать задания для программ, команд и сценариев на основании расписания. При помощи этой утилиты вы можете создавать как простые, так и сложные задания, причем они могут быть назначены на однократный поминутный запуск, а также на запуск через указанный интервал, при загрузке системы, при входе в систему, запуске службы или выполнении указанного события и прочее. Использование этой утилиты рассматривается в следующем разделе.

Возможности утилиты Schtasks.exe

Утилита командной строки SchTasks.exe позволяет выполнять те же самые операции, что и оснастка **«Планировщик заданий»**. Эти оба средства управления назначенными заданиями взаимозаменяемы, что позволяет видеть в оснастке **«Планировщик заданий»** все задания, созданные при помощи утилиты командной

строки SchTasks.exe и наоборот. Для того чтобы воспользоваться данным функционалом, вам нужно открыть командную строку, ввести команду Schtasks и указать подкоманды с соответствующими значениями.

Данная утилита включает в себя несколько подкоманд, что позволяет гибко управлять назначенными заданиями, а именно:

- Schtasks /Query
- Schtasks /Create
- Schtasks /Change
- Schtasks /Run
- Schtasks /End
- Schtasks /Delete

В следующем разделе вы познакомитесь с поднабором команд, предназначенным для отображения назначенных заданий на локальном или удаленном компьютере.

Отображение назначенных заданий. Команда Schtasks /Query

Используя команду Schtasks /query, вы можете просмотреть список назначенных заданий на локальном или удаленном компьютере. Синтаксис команды очень простой и удобный:

SchTasks /Query [/S Компьютер /U /P] [Дополнительные параметры]

Доступны следующие параметры:

- **/S**. Этот параметр отвечает за удаленную систему, для которой вы хотите просмотреть список назначенных заданий. После данного параметра вам нужно указать имя компьютера или его IP-адрес. Если параметр /S не будет указан, то по умолчанию выведется список назначенных заданий для локального компьютера;
- **/U**. При помощи этого параметра вы можете указать учетную запись пользователя, для которого будет выполняться вывод назначенных заданий. Вы можете указывать как учетные записи пользователей, расположенных в рабочих группах, так и пользователей, которые входят в состав домена;
- **/P**. Используя данный параметр, вы можете указать пароль для учетной записи, указанной при помощи параметра /U. Данный параметр не обязателен. В том случае, если вы не указали пароль, но пароль применяется

для указанной учетной записи, утилита командной строки запросит ввод пароля для продолжения действий;

– **/FO**. По умолчанию, команда /query отображает список назначенных заданий в виде таблицы со столбцами «Имя задачи», «Время следующего запуска» и «Состояние». Используя данную команду, вы можете изменить формат вывода данных. Помимо таблицы, вы можете формировать вывод данных в виде списка или файла со значениями строк разделенными запятыми (формат CSV);

– **/NH**. Данный параметр можно применить только в том случае, если данные команды выводятся в табличном формате. Эта команда указывает на то, что при выводе данных в таблице не будут отображаться заголовки столбцов.

– **/V**. Вывод данных в виде списка или файла CSV наилучшим образом сочетается с параметром /V (Verbose), что позволяет отобразить подробную информацию о каждом свойстве заданий.

Создание назначенных заданий.

Команда Schtasks /Create

Поднабор команд Schtasks предназначен для создания заданий по расписанию и таких триггеров, как запуск, вход в систему и системное событие. Эта команда поддерживает около двадцати команд, которые будут рассмотрены ниже. Для облегчения понимания материала, при описании параметров, я буду приводить примеры из оснастки **«Планировщик заданий»**.

Общие настройки задания

Первым шагом при создании любого задания является назначение заданию имени и выбор компьютера, на котором будет выполняться данное задание. Также на первом шаге создания задания вы можете указать контекст, а также выбор учетной записи, для которой будет выполняться указанное задание.

Для указания этих параметров, команде /create используются следующие параметры:

/TN. Данный параметр является обязательным и отвечает за наименование задания. По умолчанию задания создаются в папке **«Библиотека планировщика заданий»**. Для того чтобы создать задание в другой папке вам нужно ввести обратный слеш, имя папки, снова указать слеш, а затем ввести название задания, например, **«MicrosoftWindowsDefrag»**. В одной папке невозможно создать

несколько заданий с одинаковыми именами, поэтому при попытке создания задания с именем, которое уже присутствует в указанной папке, утилита Schtasks выдаст предупреждение, предлагающее заменить существующее задание. Для того чтобы заменить существующее задание нажмите на клавишу **«Y»**. В противном случае введите **«N»**.

/S. Используя этот параметр команды, вы можете создать задание на удаленном компьютере. При создании задания на удаленном компьютере нужно обратить внимание на то, что ваш и удаленный компьютеры должны быть расположены в одной рабочей группе или в одном домене. После данного параметра вам нужно указать имя компьютера или его IP-адрес.

/U. Этот параметр отвечает за учетную запись пользователя, чьи разрешения будут задействованы во время выполнения задания. Вы можете указать как учетную запись пользователя, которая находится в рабочей группе, так и пользователя, который входит в состав домена. В случае с доменной учетной записью, вам нужно сначала ввести домен, а затем учетную запись пользователя (например, testdomain.comDImaN);

/P. При помощи этого параметра вы можете указать пароль для пользовательской учетной записи. В том случае, если вы не указали пароль, но пароль применяется для указанной учетной записи, утилита командной строки запросит ввод пароля для продолжения действий;

/RU. Данный параметр указывается для того, чтобы задание выполнялось под определенной учетной записью. Если вы хотите, чтобы задание было выполнено под системной учетной записью, то в качестве значения данного параметра укажите **«»**, **«NT AUTHORITYSYSTEM»**, **«NT AUTHORITYLOCALSERVICE»**, **«NT AUTHORITYNETWORKSERVICE»** или **«SYSTEM»**;

/RP. При помощи этого параметра вы можете указать пароль для пользовательской учетной записи, указанной параметром **/RU**. В том случае, если вы не указали пароль, но пароль применяется для указанной учетной записи, утилита командной строки запросит ввод пароля для продолжения действий;

Управление триггерами при помощи командной строки

Как при помощи графического интерфейса, так и средствами командной строки, вы можете управлять всевозможными триггерами, которые предназначены для расписания выполняемого задания.

При помощи командной строки вы можете указать следующие параметры со значениями, предназначенные для расписания выполняемого задания:

Параметры /SC и /MO. Это основные обязательные параметры, которые следует указывать при создании задания. Параметр **/SC** отвечает за само расписание задания. При помощи данного параметра вы можете указать частоту повторения задания. Параметр **/MO** – это необязательный модификатор, при помощи которого выполняется контроль за периодичностью выполнения данного задания. В зависимости от значения параметра **/SC** задаются значения для параметра **/MO**. Для этих двух параметров доступны следующие значения:

- **ONCE**. Это значение параметра **/SC** позволяет запустить задание только один раз в указанные параметрами **/SD** и **/ST** дату и время. При данном значении параметр **/MO** указывать не нужно;
- **ONSTART**. Данное значение позволяет запускать задание при загрузке операционной системы. При указании данного значения, в параметре **/MO** нет необходимости;
- **ONLOGON**. При указании этого значения для параметра **/SC**, задание выполняется при входе пользователя в систему. Так же, как и с предыдущими двумя значениями, параметр **/MO** не нужно указывать;
- **ONIDLE**. Этот параметр отвечает за выполнение задания в том случае, если система находится в простое в течение заданного времени. Вместо параметра **/MO** вам нужно указать параметр **I**, описание которого вы найдете ниже;
- **MINUTE**. Указав это значение для параметра **/SC**, вы можете назначить запуск задания через определенный интервал времени, указанный в минутах. По умолчанию, задание будет выполняться один раз в минуту, но вы можете изменить расписание, используя параметр **/MO**. Значением модификатора параметра **/MO** может быть число, которое находится в интервале от 1 до 1439;
- **HOURLY**. Используя это значение, задание будет постоянно выполняться через указанный промежуток времени в часах. Так же, как и с предыдущим значением, по умолчанию задание будет выполняться один раз в час. Расписание данного задания вы можете изменить при помощи параметра **/MO**, модификатор которого может быть от 1 до 23;
- **DAILY**. Это значение указывает на то, что задание будет выполняться с периодичностью, указанной в днях. Модификатор параметра **/MO** может быть

указан в интервале от 1 до 365. По умолчанию задание будет выполняться ежедневно;

– **WEEKLY**. Данным значением параметра **/SC** вы можете указать расписание запуска задания в разрезе недели календарного года, а также указав определенные дни недели. Значениями модификатора параметра **/MO** может быть число от 1 до 52. Для того чтобы указать дни недели, вам нужно воспользоваться параметром /D, который рассматривается ниже;

– **MONTHLY**. Указав данное значение параметра **/SC**, назначенное задание будет запускаться каждый месяц или в каждый указанный день месяца. Вы можете указать параметр **/MO** со значением модификатора от 1 до 12 (в зависимости от месяца) и, указав день недели, используя параметр **/D**, определившись с датой запуска. Также вы можете комбинировать параметры **/MO** и **/M** для указания даты. Используя параметры **/D /M LASTDAY**, задание будет выполнено в последний день месяца. Также вы можете указать месяц, используя параметр **/M**, неделю месяца при помощи параметра **/MO** со значениями **FIRST, SECOND, THIRD, FOURTH** или **LAST**, а так же день недели при помощи параметра **/D**.

/D. Этот параметр отвечает за день недели, на который запланировано выполнение назначенного задания. Доступны следующие значения данного параметра: **MON, TUE, WED, THU, FRI, SAT, SUN**. Указывать значения вы можете списком, разделяя их запятыми или через дефис, что указывает на последовательность дней. Символ * задает все дни недели.

/M. Подобно дням недели, у вас есть возможность указывать месяцы календарного года. Доступны следующие значения: **JUN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV** и **DEC**. Также, как и со значениями дней недели, вы можете указывать месяцы, разделенные запятыми, например **MAR, JUN, OCT, DEC**, а также последовательность – **APR-NOV**.

/I. Используя данный параметр, вы можете указать интервал простоя системы, который необходимо выждать, прежде чем запустить запланированную задачу, для которой значением параметра **/SC** является **ONIDLE**. Вы можете указать значение интервала простоя от 1 до 999 минут.

/ST. Этот параметр отвечает за время запуска назначенной задачи. Для указания времени начала задачи используется 24-часовой формат, например, 21:54. Если данный параметр не указан, то для старта задания назначается текущее время.

Данный параметр необходимо указывать, если значением параметра /SC является ONCE.

/SD. Используя этот параметр, вы можете указать дату первого запуска назначенного задания, используя стандартный формат операционной системы, например ДД/ММ/ГГГГ. В том случае, если этот параметр не был указан, датой первого запуска задания назначается текущее число. Вы можете использовать этот параметр только со значениями **MINUTE, HOURLY, DAILY, WEEKLY** и **MONTHLY** параметра **/SC**

/ED. Текущий параметр позволяет указать дату завершения задания в стандартном формате операционной системы.

Указание действия для назначенного задания

Все вышеперечисленные задания ничего не значат без указания основного параметра – исполняемой задачи. В оснастке **«Планировщик заданий»**, исполняемую задачу вы можете указать на вкладке **«Задание»**.

За добавление исполняемой задачи в утилите командной строки SchTasks отвечает параметр **/TR**.

/TR. При помощи данного параметры вы должны указать путь и имя файла программы или скрипта, который будет выполняться с указанными требованиями. Если вам нужно указать аргументы для программы или скрипта, укажите их в пути к исполняемому файлу. Все аргументы, которые содержат пробелы, должны быть заключены в кавычки для интерпретации как один аргумент программы. Каждое задание позволяет запускать только одну программу, но используя пакетные файлы, вы можете запускать столько приложений, сколько вам нужно.

Изменение назначенных заданий.

Команда SchTasks /Change

Иногда после создания назначенного задания, скажем, во время тестирования, вы можете обнаружить, что при его создании вами была допущена ошибка. Изменить запускаемую программу, учетную запись пользователя или пароль, использующийся запланированной задачей можно, используя функционал утилиты

командной строки **SchTasks**. Для этого вам нужно воспользоваться контекстом **/Change**. Синтаксис данной команды довольно простой:

SchTasks /CHANGE [/S [/U [/P]]] [/RU] [/RP] [/TR] /TN %имя_задания%

Вы можете воспользоваться тремя параметрами, для того чтобы указать имя компьютера, пользователя и пароль для указанной вами учетной записи – параметры **/S**, **/U**, **/P**. Обязательным параметром данного контекста является параметр **/TN**, при помощи которого вы указываете название изменяемого задания. Необязательные параметры **/RU** и **/RP** определяют учетную запись, под которой будет выполняться данное задание.

Удаление назначенных заданий.

Команда SchTasks /Delete

Функционал планировщика заданий и утилиты командной строки **SchTasks** позволяет вам автоматизировать большинство рутинных задач. И вполне очевидно, что рано или поздно вам понадобится удалить какое-либо созданное ранее задание.

Утилита командной строки **SchTasks** позволяет вам удалять любое задание по имени на локальном или удаленном компьютерах. Для выполнения этих действий вы можете воспользоваться контекстом **/Delete**. Вместе с данным контекстом можно использовать любой из пяти следующих параметров:

– **/S**. Также как и во всех контекстах, которые были рассмотрены ранее, данный параметр предназначен для определения удаленного компьютера, на котором будет удаляться выбранное вами задание;

– **/U**. Данный параметр отвечает за учетную запись пользователя, в которой будет удалено данное задание;

– **/P**. Используя этот параметр, вы можете указать пароль для учетной записи, которая была вами определена параметром **/U**;

– **/TN**. При помощи текущего параметра, вы можете указать название задания, которое будет удалено. Если вы хотите удалить все задания, то вместо названия укажите *;

– **/F**. Этот параметр позволяет вам выполнить форсированное удаление задания, иными словами, принудительное удаление с подавлением всех сообщений.

Запуск назначенного задания.

Команда SchTasks /Run

Иногда бывают такие случаи, когда вам нужно выполнить действие, которое было создано в задании немедленно, несмотря на то, что время запуска еще не наступило. Это можно сделать, используя функционал утилиты **SchTasks**. Для запуска задания средствами командной строки вам нужно воспользоваться контекстом **/Run**. Запуск задания не влияет на его расписание и не изменяет время следующего запуска. Набор параметров для этого контекста невелик. Вы можете указать имя удаленного компьютера, учетную запись пользователя под которым будет выполняться задание, а также пароль к этой учетной записи, используя уже известные вам параметры **/S**, **/U** и **/P**. Параметр **/TN** позволяет вам указать название задания, которое необходимо запустить.

Остановка выполняемого задания.

Команда SchTasks /End

В некоторых случая при выполнении задач, которые занимают много времени, вам может понадобиться остановить выполняемое задание. Остановка задания, так же как и немедленный запуск, не повлияют на его дальнейшее расписание. Утилита командной строки **SchTasks** поддерживает данную функцию. Для этого вы можете воспользоваться контекстом **/End**. Для этого контекста можно использовать четыре основные команды, которые рассматривались в каждом из предыдущих контекстов – **/S**, **/U**, **/P**, а также **/TN**, при помощи которого вы можете указать название останавливаемого задания, которое на данный момент выполняется.

8.2. Порядок выполнения практической работы

Задание 8.1. Работа с планировщиком заданий с использованием средств командной строки.

ВНИМАНИЕ! Перед началом выполнения задания обязательно задайте пароль пользователю, под именем которого Вы работаете.

1. Создайте задание, которое выполниться только один раз:

2. Создайте задание, которое будет выполняться при загрузке операционной системы

3. Создайте задание, которое будет запускаться при входе пользователя в систему, например, будет проводиться дефрагментация диска.

4. Если система будет находиться в простое на протяжении 10 минут, то будет запускаться «Системный монитор».

5. Создайте задание, при помощи которого у вас раз в каждые три часа будет запускаться игра «Сапер».

6. Создайте задачу, используя которую, при каждом включении компьютера будет открываться блокнот.

7. Выведите назначенные задачи для локального компьютера в табличном формате без наименований столбцов:

8. Выведите назначенные задачи для локального компьютера в виде списка с подробной информацией о каждом значении:

9. Измените задачу, созданную в пункте 6 таким образом, чтобы вместо блокнота запускался WordPad.

10. Удалите задачу, созданную в пункте 4.

11. Запустите вне расписания задачу, созданную в пункте 3.

12. Остановите запущенную в предыдущем пункте дефрагментацию, не дожидаясь ее окончания

9. Аудит системных процессов и событий в ОС Windows XP

Цель работы: Создание пользовательской консоли администрирования MMC, выполняющей функции аудита системных процессов и событий в ОС Windows XP.

9.1. Краткие теоретические сведения

I. В 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 XP 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 XP, 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. 9.1. Дополнительная информация по данной тематике доступна в соответствующих разделах справки ОС Windows XP **(Пуск | Справка и поддержка)**.

9.2. Порядок выполнения практической работы

Задание №9.1. Изучить основные возможности оснасток, предназначенных для обеспечения аудита системных процессов и событий в ОС Windows XP на конкретных примерах.

Секция А. Ознакомление с основными возможностями оснастки «Групповая политика», предназначенными для функций аудита ОС Windows XP.

Таблица 9.1. Основные события аудита в ОС Windows XP

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

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

Для ознакомления с возможностями оснастки «Групповая политика» выполните следующее.

1. Локально добавьте на вновь созданную консоль администрирования, системную оснастку **«Редактор объекта групповая политика»**.

2. 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.

3. 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.

4. Настройте аудит файлов и папок. Для этого измените параметры **«успех»** или **«отказ»** категории событий **«Аудит доступа к объектам»**.

Выберите папку для аудита. Если в **«Свойствах»** объекта отсутствует вкладка **«Безопасность»**, 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 **ОК**;

– 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)»**.

Далее 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 ОК 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 **ОК** и **Применить** для подтверждения ввода.

5. Не закрывая консоль администрирования ММС, сохраните ее.

Секция В. Ознакомление с основными возможностями оснастки **«Просмотр событий»** в ОС Windows XP.

В предыдущей секции был изучен вопрос организации и настройки аудита системных событий различных категорий, в частности, событий, связанных с обеспечением безопасности ОС. Однако помимо указанных в ОС Windows XP дополнительно имеются события других категорий, например, события, связанные с работой приложений и программ. Поскольку, аудит предполагает регистрацию различного рода системных событий (табл. 9.2), имеющих место в операционной среде, их регистрация в ОС Windows XP осуществляется в журналах трех основных типов, описание которых представлено после таблицы. В 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. В 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. В дополнение к существующим ОС Windows XP 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 9.2. Типы системных событий в ОС Windows XP

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

В журнале службы каталогов содержатся события, заносимые службой каталогов ОС Windows XP. 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 XP. 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 хранится серверная копия общих файлов, реплицируемых между всеми контроллерами домена. Кроме того, существует журнал DNS-сервера, в который записываются сообщения о системных событиях, зарегистрированных службой DNS. В этот журнал записываются события, связанные с разрешением DNS-имен IP-адресам.

В ОС Windows XP 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. 9.1), воспользовавшись компонентом **«Групповая политика»**. В настоящей секции предполагается изучить основные возможности регистрации системных событий различных категорий посредством имеющегося в ОС Windows XP служебного инструмента – оснастки **«Просмотр событий»**.

Для ознакомления с возможностями данной оснастки выполните следующее.

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. 9.2). 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 **Приложение** событие **«Уведомление»** за прошедшее время,

– в журнале **Безопасность** событие **«Аудит отказов»**,

– в журнале С**истема** событие **«Ошибка»** за последние 30 минут, с сортировкой по времени «от новых к старым».

4. В окне журнала событий системы удалите столбцы **«Пользователь»**, **«Компьютер»** и **«Категория»**, оставив остальные.

5. Воспользовавшись системой поиска, найдите событие типа **«Уведомление»** с кодом **1800** от источника **SecurityCenter** в журнале **Приложение**.

6. 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**.

7. Не закрывая консоль администрирования ММС, сохраните ее.

10. Подсистема безопасности (квотирование, шифрование, доступ к объектам)

Цель работы: изучение базовых возможностей обеспечения безопасности объектов файловой системы NTFS в среде ОС Windows XP.

10.1. Краткие теоретические сведения

В современных условиях развития сети Интернет как глобального средства коммуникации обеспечение безопасности данных в коммерческой организации становится все более актуальной задачей, возлагаемой, главным образом, на системного администратора. В связи с учащающимися случаями проникновения в незащищенные сети, атаками и просто потенциальными угрозами инструментарий профессионала в области информационной безопасности должен быть максимально широким и включать все возможные аппаратно-программные средства защиты (аппаратные и программные сетевые экраны, брандмауэры, аппаратные и программные средства ограничения локального и удаленного доступа, управления локальной и групповой политикой), а не ограничиваться антивирусными пакетами на защищаемых узлах сети. Большинство программных компонентов для решаемых задач безопасности доступны системному администратору сразу же после установки сетевой операционной системы, в частности, ОС Windows XP. При этом принципиальных отличий в настройке элементов безопасности локального узла или сервера домена не существует, поскольку безопасность в сети подчиняется единому набору правил, называемому политикой безопасности организации.

Таким образом, при создании сети на базе ОС Windows XP безопасность необходимо обеспечивать на двух уровнях: на уровне локального компьютера и на сетевом, уровне домена или рабочей группы. Программные средства профессиональной версии ОС Windows XP позволяют обеспечивать безопасность несколькими способами. Часть из этих средств была унаследована от предыдущих версий операционных систем семейства Windows, другие компоненты, напротив, появились сравнительно недавно и успешно применяются.

С появлением каждой новой сетевой ОС семейства Windows средства безопасности, эволюционируя, претерпевают значительные изменения, позволяющие администратору сети гибко настраивать ее и обеспечивать, тем самым, приемлемый уровень комплексной защиты вычислительной системы.

Данное утверждение не является исключением также по отношению к изучаемой ОС Windows XP. В ней имеется ряд программных средств от ОС предыдущего поколения, ОС Windows NT и ОС Windows 2000, но имеются и новые средства обеспечения безопасности, основные из которых представлены ниже.

– *Собственность администратора*. В ранних версиях ОС Windows любые ресурсы (файлы и каталоги), созданные администратором, становились достоянием всей группы. В профессиональной ОС Windows XP ресурсы теперь принадлежат тому, кто их создал.

– *Ограничения, связанные с использованием пустого пароля*. Теперь пользователи ОС Windows XP могут использовать пустые пароли при регистрации, но с ними они могут регистрироваться локально, только физически присутствуя.

– *Программные ограничения*. Политика безопасности ОС Windows XP может быть присвоена отдельным приложениям на основании пути к исполняемому файлу (порту), Интернет-зоны или сертификата безопасности.

– *Быстрая смена пользователей*. Узлы, работающие в среде ОС Windows XP и при этом не соединенные с доменом, могут быстро переключаться с одного пользователя на другого, не выходя из локальной сети и не закрывая приложений.

– *Мастер сброса пароля*. Если пользователь забыл свой пароль, то он может воспользоваться загрузочным диском для осуществления доступа к своей учетной записи.

Нетрудно заметить, что отмеченные возможности обеспечения безопасности, как локальной, так и глобальной, стали более доступными с точки зрения их сетевого применения и практически ориентированными на гибкое администрирование и конфигурирование ОС. Это позволяет сделать вывод о том, что данная тенденция будет наблюдаться и впредь, позволяя профессионалам постоянно иметь необходимый инструментарий.

В первом приближении некоторые вопросы обеспечения локальной безопасности уже имели место в предыдущих лабораторных работах. В частности, было осуществлено знакомство с одним из основных инструментов системного администратора, консолью администрирования MMC и одной из основополагающих оснасток «Групповая политика», являющейся обязательной для целей конфигурирования безопасной операционной среды.

В рамках настоящей практической работы и соответствующей лабораторной работы предполагается изучить дополнительные инструменты системного

администратора и выполнить ряд мероприятий, направленных на обеспечение сетевой безопасности, а именно осуществить некоторые элементарные действия по управлению локальной политикой безопасности, рассмотреть процедуру безопасного входа в систему, организовать аудит в журналах безопасности Internet Connection Firewall, поговорить о шаблонах безопасности, а также научиться анализировать и конфигурировать подсистему безопасности ОС в целом. Отдельно предполагается рассмотреть вопросы, связанные с обеспечением безопасности файловой системы, ее объектов (файлов и каталогов) как локально, так и при сетевом взаимодействии.

Термины FAT и NTFS являются общими названиями файловых систем (ФС), каждая из которых включает в себя несколько различных модификаций. Например, имеются следующие разновидности ФС FAT: FAT12, FAT16 и FAT32 и, напротив, существует две версии ФС NTFS – v.4.0 и v.5.0.

Если ранее в ОС Windows NT использовалась ФС NTFS v.4.0, то ОС Windows XP предлагает самую последнюю версию ФС NTFS – v.5.0, представленную еще в ОС Windows 2000. Хотя ФС обеих версий приспособлены к взаимному чтению и записи объектов (файлов и каталогов), в ОС Windows XP имеется ряд преимуществ, которыми ОС Windows NT не наделена. К их числу, например, относятся:

– возможности создания "точек повторной обработки", которыми ОС Windows NT не в состоянии воспользоваться при обращении к жесткому диску с ОС Windows XP;

– также, ОС Windows NT будет игнорировать квоты дискового пространства, установленные под управлением ОС Windows XP;

– кроме того, ОС Windows NT в отличие от ОС Windows XP не сможет ни читать, ни делать запись в шифрованных файлах;

– . и наконец, ОС Windows NT будет игнорировать журнал изменений, доступный в ОС Windows XP.

Указанные особенности делают ФС NTFS v.5.0 мощным инструментом безопасности с встроенными возможностями администрирования, который при правильном применении обеспечивает более продуктивную и эффективную организацию системы. Это обстоятельство выгодно отличает данную ФС от ее предыдущей версии и, тем более, от ФС FAT, в сравнении с которой также имеется ряд отличительных особенностей:

– ФС NTFS обеспечивает безопасность на уровне файлов, в отличие от общей безопасности ФС FAT;

– при помощи ФС FAT имеется возможность запретить или разрешить доступ из сети к части дискового пространства, в то время как с помощью ФС NTFS можно установить доступ к конкретным объектам (файлам и каталогам);

– ФС NTFS тесно взаимосвязана с подсистемой безопасности ОС, в целом, и взаимодействует с подсистемой безопасности сети, в частности.

Известно, что "памяти никогда не бывает много!". Это утверждение в полной мере относится к внешней памяти жесткого диска. В этой связи администратору сетевых ресурсов необходимо контролировать расход доступной в его распоряжении внешней памяти. В ФС NTFS имеется штатное программное средство, позволяющее это делать – оно позволяет ограничивать свободное пространство на жестком диске, предполагаемое к выделению пользователям.

Процесс выделения пользователю определенного объема внешней памяти жесткого диска называется квотированием, а сам выделяемый объем, соответственно, квотой на дисковое пространство. Квотирование дискового пространства в организации необходимо с целью его безопасного расходования. Если свободное пространство на жестком диске ограничено, квоты помогут избежать потери исключительно важных данных, которые просто могут не уместиться на заполненный до отказа диск.

В ОС Windows XP квотирование дискового пространства позволяет выполнять следующие действия.

– Уведомлять пользователя о том, что он превысил порог выдачи предупреждения (но при этом еще не израсходовал свою квоту).

– Не допускать запись на жесткий диск после того, как пользователь исчерпал отведенную ему квоту.

Квотирование диска работает индивидуально в отношении каждого пользователя и каждого тома. При этом квоты "прозрачны" для пользователя. Когда он смотрит на доступное пространство диска, то видит, сколько осталось от выделенной ему части. После исчерпания квоты на диске, дальнейшее сохранение данных невозможно. В этом случае пользователь может удалить объекты (файлы и каталоги) или передать их в собственность другого пользователя, чтобы освободить дисковое пространство, или же попросить сетевого администратора об увеличении квотируемого объема.

При установлении пользователям квот необходимо помнить несколько принципиальных моментов. Квотируемый жесткий диск должен быть отформатирован в ФС NTFS. Лицо, выдающее квоты, должно иметь полномочия администратора. Порог выдачи предупреждения должен быть процентов на десять меньше, чем сама квота. Например, квота в 1Гб должна сопровождаться порогом выдачи предупреждения в 900Мб. Когда пользователь израсходует выделенные 900Мб, в регистрационном журнале будет сделана соответствующая запись; когда порог квотирования в 1Гб будет превышен, осуществляется запрет на дальнейшее использование жесткого диска и также делается соответствующая запись в журнале регистрации.

10.2. Порядок выполнения практической работы

Для ознакомления с возможностями квотирования дискового пространства в среде ОС Windows XP выполните следующее.

Задание №10.1. Изучение возможностей квотирования дискового пространства в среде ОС Windows XP на конкретных примерах.

Секция А. Активация возможности квотирования локального тома в среде ОС Windows XP.

1. Из контекстного выпадающего меню **"Свойства"** тома выберите вкладку **"Квота"**, на которой установите флажок рядом с надписью **"Включить управление квотами"**, тем самым, активизировав изучаемую функциональность.

2. Установите квоту в 1Гб и порог предупреждения в 900Мб, выделяемые по умолчанию для каждого нового пользователя квотируемого жесткого диска.

3. Задействуйте протоколирование превышение порога предупреждения и выделенной квоты в журнале регистрации.

4. Нажмите ОК, чтобы изменения вступили в силу.

Примечание. Уместно отметить, что выделение квот возможно не только для локальных пользователей, но и для удаленных. При этом обязательным условием, помимо указанных выше, должно быть то, что общим для доступа каталогом должен быть корневой каталог квотируемого тома.

Секция В. Протоколирование и управление квотами локального тома в среде ОС Windows XP.

После того, как дисковые квоты установлены, появляется возможность отслеживать пороги квот, статус предупреждения или реально использованное пространство.

1. Просмотрите выделенные пользователям квоты. Для этого манипулятором мышь щелкните на кнопке **"Записи квот"** и изучите появившийся список существующих в системе пользователей и выделенные им квоты. Обратите внимание на то, что в списке пользователей имеется учетная запись системной группы "Администраторы", у которой предельные значения порога превышения и самой квоты отсутствуют.

Примечание. Если в момент первого запуска диалоговое окно **"Записи квот"** окажется пустым, то необходимо заполнить список пользователей, за которыми предстоит вести наблюдение и протоколирование расхода их дискового пространства.

2. Введите в список нового пользователя, которому необходимо выделить квоту. Для этого в меню **"Квота"** на панели инструментов выберите команду **"Создать запись квоты..."**, а затем в появившемся окне добавьте стандартным способом соответствующего пользователя (в качестве примера можно взять пользователя с именем "Гость"). Обратите внимание на то, что в процессе создания новой записи квоты, имеется возможность установить особые значения предельных параметров порогового значения и самой квоты для данного пользователя.

В меню **"Квота"** также имеется возможность удалить ненужные записи. В случае необходимости удалите ненужного пользователя из сформированного списка. Это делается простым выбором команды **"Удалить запись квоты..."**.

3. Теперь предположим, что некоторому пользователю (например, с именем "Гость") требуется выделить дополнительное пространство на жестком диске. Для изменения его квоты необходимо в окне "Записи квот" правой кнопкой манипулятора мышь щелкнуть на его записи, выбрать команду **"Свойства"** и установить новые значения параметров в появившемся окне.

4. Закройте диалоговое окно **"Записи квот"** и нажмите **ОК**, чтобы изменения вступили в силу.

При выполнении заданий секций используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №10.2. Изучение основных возможностей файловой системы EFS в среде ОС Windows XP на конкретных примерах.

Использование ФС **EFS** (Encrypting File System – шифрующая файловая система) в ОС Windows XP представляет собой дополнительную возможность защиты данных на жестком диске. При применении ФС EFS сохраняемые на диске файлы шифруются и становятся недоступными, пока к ним не будет обеспечен корректный доступ в рамках NTFS-тома.

При работе с ФС EFS лучше всего зашифровывать целый каталог, а не отдельные файлы. Это ускоряет процесс и делает его более эффективным. Таким образом, появляется возможность создать защиту группы файлов вместо шифрования отдельных из них. При шифровании каталога целиком все запасные копии файлов также шифруются (разумеется, только в том случае, если они хранятся в шифруемом каталоге).

Для ознакомления с возможностями ФС EFS в среде ОС Windows XP выполните следующее.

1. Войдите в систему под любой учетной записью (стандартной или созданной заранее).

2. В служебном программном модуле **"Мой компьютер"** (**Пуск | Мой компьютер**) создайте самостоятельно каталог и скопируйте в него какой-либо файл, предполагаемый к шифрованию.

3. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **"Свойства"** из контекстного выпадающего меню.

4. На вкладке **"Общие"** появившегося диалогового окна щелкните на кнопке **"Дополнительно"** (или **"Другие"**) и установите флажок рядом с надписью **"Шифровать содержимое для защиты данных"**.

5. Нажмите **ОК** для подтверждения операции.

Примечание. После шифрования объект будет выделен зеленым цветом.

6. Войдите в систему под другой учетной записью и произведите открытие файла. Обратите внимание на полученный результат.

Примечание. Расшифровывание объектов возможно в обратном порядке и под той учетной записью, в рамках которой происходило шифрование.

При выполнении задания используйте следующие инструкции:

– перенесите последовательность выполняемых действий в отчет (возможно приведение графических фрагментов, сделанных с экрана, в качестве демонстрационного материала),

– сделайте вывод о проделанной работе и запишите его в отчет.

Задание №10.3. Изучение основных возможностей доступа к объектам в среде ОС Windows XP на конкретных примерах.

ОС Windows XP позволяет реализовать совместное использование файлов, папок, принтеров и других сетевых ресурсов. С этими ресурсами могут работать либо другие пользователи локального компьютера, либо пользователи, находящиеся в сети. То, каким образом ресурсы используются совместно, зависит от настройки системы.

Совместное использование на уровне каталога является базовым уровнем, на котором можно осуществлять управление. Совместное использование одного файла невозможно реализовать в ОС Windows XP. Файл должен быть перенесен или создан внутри папки, предназначенной для совместного использования.

Для совместного использования ресурсов в сети сначала необходимо инициировать службу доступа к файлам и принтерам сетей Microsoft (File and Printer Sharing for Microsoft Networks). Если отсутствует вкладка **"Доступ"** в диалоговом окне свойств папки, то указанная служба не подключена.

Поскольку данная служба, как правило, устанавливается в автоматическом режиме в процессе установки ОС, ее ручное инсталлирование не представляется к рассмотрению в рамках практической работы (инструкция по процедуре ручного добавления данной службы доступна в центре справки и поддержки ОС, а также на специализированных ресурсах глобальной сети).

ОС Windows XP предлагает пять уровней доступа к объектам (файлам и каталогам) ФС NTFS, которые необходимо знать и разделять, чтобы корректно

настраивать параметры безопасности в соответствии с потребностями организации при совместном использовании сетевых ресурсов. Каждый из указанных уровней доступа рассматривается далее в соответствующей секции текущего задания лабораторной работы.

Внимание! Дальнейшее конфигурирование параметров безопасности показано на примере ОС с подключенной опцией **"Простой общий доступ к файлам"** (**"Пуск | Панель управления | Свойства папки", вкладка "Вид", окно "Дополнительные параметры"**).

Секция А. Изучение первого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Первый уровень (**Уровень I**) доступа является самым строгим в ФС NTFS: только владелец объекта может читать и модифицировать его. Другие пользователи, включая сетевого администратора, не имеют доступ к таким объектам. Все объекты в каталоге с первым уровнем доступа сохраняют тот же уровень секретности, что и родительский каталог.

Примечание. Возможность создания каталога Уровня I доступна только для учетной записи группы "Пользователи" и только в рамках его собственной папки "Мои документы".

Для обеспечения доступа Уровня I необходимо выполнить следующее.

1. Одним из ранее изученных способов создайте новую учетную запись пользователя с правами группы "Пользователи" или воспользуйтесь уже готовой учетной записью, полученной в предыдущих заданиях.

2. Войдите в систему с правами группы "Пользователи", воспользовавшись только что созданной учетной записью, и создайте в служебном каталоге **"Мои документы"** (расположен в соответствующем профиле учетной записи) новый подкаталог с именем, выбранным самостоятельно.

3. Установите **"Простой общий доступ к файлам"**, как указано выше.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду "Общий доступ и безопасность" из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **"Доступ"** установите флажок рядом с надписью **"Отменить общий доступ к этой папке"** в категории доступа **"Локальный общий доступ и безопасность"**.

6. Нажмите **"Применить"** (в случае необходимости установите новый пароль на текущую учетную запись) и **ОК** для подтверждения операции.

7. Войдите в систему под любой другой учетной записью (в том числе и с правами администратора) и убедитесь, что созданный каталог является недоступным для открытия, тем самым, обеспечивая конфиденциальность сохраненных в нем данных.

Секция В. Изучение второго уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

На втором уровне (**Уровень II**) владелец файла и администратор имеют права на чтение и запись в файле или каталоге. В ОС Windows XP это является настройкой по умолчанию для каждого пользовательского файла в служебном каталоге **"Мои документы"**.

Для обеспечения доступа Уровня II необходимо выполнить следующее.

1. Одним из ранее изученных способов создайте новую учетную запись пользователя с правами группы "Пользователи".

2. Войдите в систему с правами группы "Пользователи", воспользовавшись только что созданной учетной записью, и создайте в служебном каталоге **"Мои документы"** (расположен в соответствующем профиле учетной записи) новый подкаталог с именем, выбранным самостоятельно.

3. Установите **"Простой общий доступ к файлам"**, как указано выше, если он еще не был установлен.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **"Общий доступ и безопасность"** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке "**Доступ"** удалите флажки рядом с надписью **"Отменить общий доступ к этой папке"** в категории доступа **"Локальный общий доступ и безопасность"** и надписью **"Открыть общий доступ к этой папке"** в категории доступа **"Сетевой общий доступ и безопасность**", если они находятся в установленных положениях.

6. Нажмите **OK** для подтверждения операции.

7. Войдите в систему под любой другой учетной записью кроме административной (если необходимо, создайте еще одну с правами пользователя) и убедитесь, что созданный каталог является недоступным для удаления и модификация его содержимого невозможна.

8. Войдите в систему под учетной записью с правами администратора и убедитесь, что он имеет доступ к вновь созданной папке на чтение и запись.

Секция C. Изучение третьего уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Третий уровень (**Уровень III**) позволяет пользователям, входящим в систему из локальной сети, совместно использовать объекты ФС NTFS (файлы и каталоги). В зависимости от типа пользователя ему позволено или запрещено выполнять определенные действия с файлами Уровня III в каталоге "Общие документы". В частности,

– администраторы локальных компьютеров и опытные пользователи имеют полный доступ,

– ограниченные пользователи имеют доступ "только для чтения",

– удаленные пользователи не имеют доступа к файлам Уровня III.

Для обеспечения доступа Уровня III необходимо выполнить перемещение желаемого объекта файловой системы в каталог **"Общие документы"**. Выполните следующее:

Воспользовавшись знаниями, полученными в предыдущих заданиях, самостоятельно создайте объект ФС NTFS с доступом Уровня III и занесите последовательность выполняемых действий в отчет.

Секция D. Изучение четвертого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Один из самых распространенных уровней сетевого доступа является **Уровень IV**. На этом уровне объекты ФС NTFS доступны для чтения всем удаленным

пользователям. Локальные пользователи также имеют право чтения (это касается и учетных записей "Гость"), но не имеют права записи и модификации объектов.

Внимание! Право организации доступа Уровня IV присвоено администратору сети.

Для обеспечения доступа Уровня IV необходимо выполнить следующее:

1. В виртуальной машине войдите в систему с правами администратора. Отключите брандмауэр и создайте в любом месте локального тома новый каталог с именем, выбранным самостоятельно, и запишите в него любой текстовый файл для дальнейших операций.

2. Установите **"Простой общий доступ к файлам"**, как указано выше, если он еще не был установлен.

3. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **"Общий доступ и безопасность"** из выпадающего контекстного меню.

4. В появившемся диалоговом окне на вкладке **"Доступ"** щелкните фразу "**Если вы понимаете потенциальную опасность, но все равно хотите включить общий доступ без помощи мастера, щелкните здесь"**.

5. Установите флажок рядом с надписью **"Открыть общий доступ к этой папке"** в категории доступа **"Сетевой общий доступ и безопасность"** и удалите флажок рядом с надписью **"Разрешить изменение файлов по сети"**, если он находится в установленном положении.

6. Нажмите ОК для подтверждения операции.

7. На физической машине нажмите **Пуск | Выполнить** и введите ***ip_адрес_виртуальной_машины***. Откройте только что созданный каталог и произведите чтение данных из текстового файла, находящегося внутри.

8. Убедитесь, что созданный каталог является недоступным для удаления и модификация его содержимого по сети невозможна.

Секция Е. Изучение пятого уровня доступа к объектам файловой системы NTFS в среде ОС Windows XP.

Второй из распространенных уровней сетевого доступа, который достаточно часто встречается при организации локальной сети, в том числе, в домашних условиях, – **Уровень V**. Этот уровень является наиболее "разрешенным" с точки зрения безопасности объектов файловой системы. Любой пользователь локальной сети может читать, записывать данные по сети, удалять файлы и каталоги, а также модифицировать их содержимое. Из этого следует, что такой уровень безопасности следует вводить только в закрытых и надежно защищенных от внешнего воздействия локальных сетях.

Внимание! Право организации доступа Уровня V присвоено администратору сети.

Для обеспечения доступа Уровня V необходимо выполнить следующее:

1. В виртуальной машине войдите в систему с правами администратора, воспользовавшись только что созданной учетной записью. Создайте в любом месте локального тома новый каталог с именем, выбранным самостоятельно, и запишите в него любой текстовый файл для дальнейших операций.

3. Установите **"Простой общий доступ к файлам"**, как указано выше, если он еще не был установлен.

4. Щелкните правой кнопкой манипулятора мышь на созданном каталоге и выберите команду **"Общий доступ и безопасность"** из выпадающего контекстного меню.

5. В появившемся диалоговом окне на вкладке **"Доступ"** установите флажок рядом с надписью **"Открыть общий доступ к этой папке"** и флажок рядом с надписью **"Разрешить изменение файлов по сети"** в категории доступа **"Сетевой общий доступ и безопасность"**.

6. Нажмите **ОК** для подтверждения операции.

7. На физической машине нажмите **Пуск | Выполнить** и введите ***ip_адрес_виртуальной_машины***. Откройте созданный администратором предыдущего узла каталог и произведите чтение данных из текстового файла, находящегося внутри.

8. Убедитесь, что созданный каталог является доступным для модификации. Для этой цели модифицируйте по сети содержимое текстового файла в каталоге с общим доступом и сохраните его.

Полученные в настоящей практической работе знания и изученные возможности снабжают потенциального системного администратора или опытного пользователя базовым инструментарием, ориентированным на обеспечение безопасности компьютера от различного рода сетевых воздействий, атак или угроз как локальных, так и внешних.

11. Базовые регулярные выражения UNIX

Цель работы: ознакомление с языком базовых регулярных выражений и командой ***grep***.

11.1. Краткие теоретические сведения

Регулярные выражения представляют собой одно из наиболее интересных и полезных свойств операционной системы UNIX. Регулярные выражения являются языком описания текстовых шаблонов, который используется во многих системных утилитах для выполнения операций поиска и отбора при разнообразных обработках текстовых строк. Мы изучим регулярные выражения на примере применения их в утилите поиска *grep*.

Утилита поиска *grep*

Синтаксис

grep [опции] [шаблон] [файл...]

Описание

Команда *grep* выполняет поиск строк, соответствующих шаблону, заданному регулярным выражением, в файлах или во входном потоке. Если команда задана без опций, выводятся все найденные строки. Если имя файла не задано, команда выполняет поиск во входном потоке. Если задано несколько имен файлов или в составе имени файла использован символ '*', *grep* перед строкой выводит имя файла, которому эта строка принадлежит.

Опции

-c	выводится только число строк файла, соответствующих шаблону
-f *файл*	чтение шаблона из *файла*
-h	не выводятся имена файлов, в которых найдены строки, соответствующие шаблону

-i	игнорирование верхнего/нижнего регистров
-l	выводятся только имена файлов, в которых найдены строки, соответствующие шаблону
-n	перед каждой выводимой строкой выводится ее номер в файле
-v	ищутся строки, не соответствующие заданному шаблону
-w	ищутся слова, полностью соответствующие шаблону
-x	ищутся строки, полностью соответствующие шаблон

Регулярные выражения

Регулярные выражения представляют собой язык описания текстовых шаблонов. Регулярные выражения содержат образцы символов, входящих в искомое текстовое выражение, и конструкции, определяемые специальными символами (метасимволами).

Метасимволы, используемые в регулярных выражениях

^	Если необходимо выбрать первые символы строки (ставится перед выражением)
$	Если необходимо выбрать последние символы строки (ставится после выражения)
[]	любой символ, заключенный в квадратные скобки; чтобы задать диапазон символов, в квадратных скобках указываются через дефис первый и последний символы диапазона
[^]	любой символ, кроме символов, заданных в квадратных скобках
.	любой отдельный символ
\	отменяет специальное значение следующего за ним метасимвола
*	указывает, что предыдущий шаблон встречается 0 или более раз
\{n\}	указывает, что предыдущий шаблон встречается ровно n раз
\{n,\}	указывает, что предыдущий шаблон встречается не менее n раз
\{,n\}	указывает, что предыдущий шаблон встречается не более n раз

\{n,m\} указывает, что предыдущий шаблон встречается не менее n и не более m раз

Примеры регулярных выражений

^the	ищутся строки, начинающиеся с буквосочетания "the"
be$	ищутся строки, заканчивающиеся буквосочетанием "be"
[Ss]igna[lL]	ищутся строки, содержащие буквосочетания: "signal", "Signal", "signaL" или "SignaL"
\.	ищутся строки, содержащие точку
^...th	ищутся строки, содержащие символы "th" в 4-й и 5-й позициях
^.\{53\}th	ищутся строки, содержащие символы "th" в 54-й и 55-й позициях
^.\{10,30\}th	ищутся строки, содержащие символы "th" в любых позициях между 10-й и 30-й включительно
^.....$	ищутся строки, состоящие из 5 любых символов
^t.*e$	ищутся строки, начинающиеся с буквы "t" и заканчивающиеся буквой "e"
[0-9][a-z]	ищутся строки, содержащие комбинацию: цифра-прописная буква
[^123]	ищутся строки, не содержащие цифр "1" или "2" или "3"

Особые указания

Перед знаками фигурных скобок { и } всегда ставится знак слэша "\", чтобы оболочка воспринимала их именно как служебный символ, внутри которого указывается какое-то условие.

Чтобы пропустить известное фиксированное количество любых символов с начала строки, выражение включает

^.{число_символов}

Чтобы пропустить известное меняющееся количество любых символов с начала строки, выражение включает

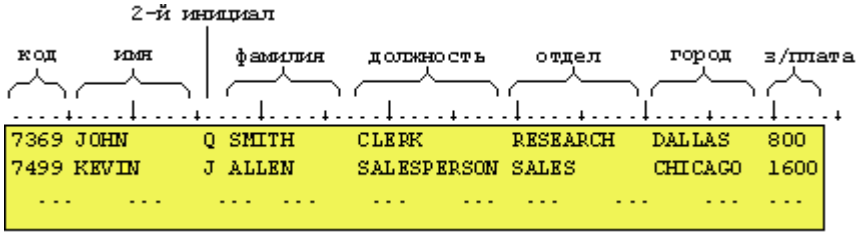
^.{минимальное_количество_символов,максимальное_количество_символов}

Чтобы выбрать любое число, выражение включает [0-9]

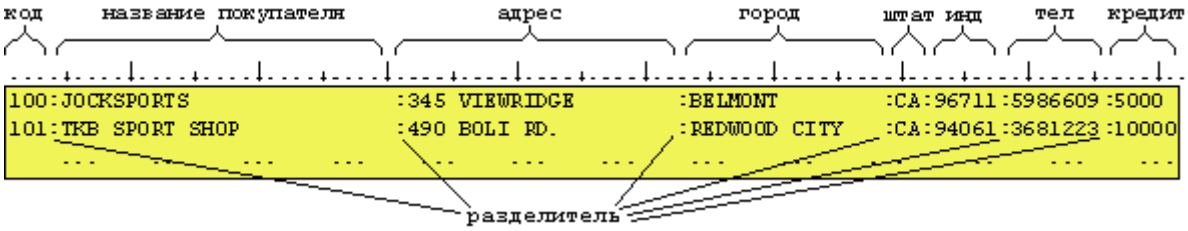
11.2. Структура файлов query 1 – query 5

Для выполнения практической работы необходимо знать структуру файлов, из которых осуществляется выборка данных. Ниже представлена структура всех файлов, необходимых для данной практической работы.

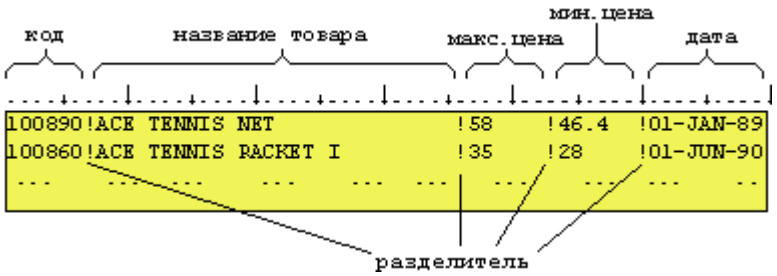
Структура файла query1



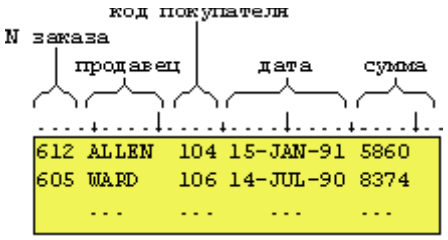
Структура файла query2



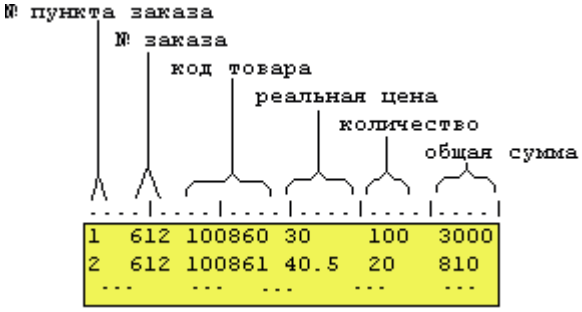
Структура файла query3



Структура файла query4



Структура файла query5



11.3. Подготовка к выполнению практической работы

ВНИМАНИЕ!!! Если не выполнить написанное в этом абзаце, то невозможно будет выполнение всей практической работы!!! Запустите виртуальную машину с гостевой операционной системой SLAX Linux (выберите SLAX graphics VESA mode). После загрузки гостевой операционной системы, на рабочем столе дважды щелкните по ярлыку **System**. В открывшемся окне выберите **Storage Media**, затем – **Floppy Drive**. Когда увидите содержимое виртуальной дискеты, закройте это окно.

11.4. Порядок выполнения практической работы

1. Откройте консоль (второй значок в виде черного прямоугольника с белой окантовкой слева внизу), перейдите в корневой каталог, откуда зайдите в подкаталог **disk** каталога **media**, где убедитесь в наличии в нем файлов с именами query 1 – query 5. Все задания необходимо выполнять, находясь в этом каталоге.

2. В файле query1 выбрать сотрудников, имеющих должность "менеджер" или "клерк" (по выбору).

3. В файле query1 выбрать все строки, в которых зарплата сотрудников равна круглому числу тысяч.

4. В файле query2 выбрать все строки, в которых в адресе имеется обозначение улицы (ST.)

5. В файле query3 выбрать все строки, в которых максимальная цена равна 20.

6. В файле query4 выбрать все строки, в которых дата продажи - весна 1990 г.

7. В файле query5 выбрать все строки, в которых указан товар, имеющий код 100860 и проданный по цене 35

ЗАКЛЮЧЕНИЕ

Методические указания для выполнения практических работ по дисциплине "Операционные системы ЭВМ" позволяет изучить практические основы настройки и администрирования операционных систем Windows семейства NT и UNIX. После выполнения всех практических работ студенты получают достаточный уровень в области работы с операционными системами. Для получения более углубленных знаний в этой сфере предлагается использовать руководство к выполнению лабораторных работ по данной дисциплине.

ЛИТЕРАТУРА

1. Танненбаум Э. Современные операционные системы. 3-е изд. – СПб.:Питер, 2010. – 1120 с.: ил. – (Серия "Классика Computer Science").

2. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – СПб.: Питер, 2002. – 544 с.: ил.

3. Руссинович М., Соломон Д. Внутреннее устройство Microsoft Windows: Windows Server 2003, Windows XP и Windows 2000. Мастер-класс. / Пер. с англ. – 4-е изд. – М.: Издательско-торговый дом "Русская Редакция"; СПб.: Питер, 2005. – 992 с.: ил.

4. Пахмурин Д.О. Операционные системы ЭВМ: Учебное пособие. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2013. – 254 с.: ил.